# Empezando a Entender las Redes de Computadoras

**Material de Resumen para el Curso de Taller de Mantenimiento de Segundo Año del Bachillerato de Informática.**

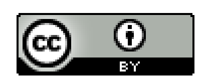
Prof. Víctor Méndez

Consejo de Educación Técnico-Profesional

Universidad del Trabajo del Uruguay

E-Mail: vicanmendez@gmail.com

2018



# Contenido


Presentación 8
Fundamentos Teóricos Básicos 9
Medios 10
Red 10
Señal 11
Comunicación 12
Dispositivos DCE y DTE 13
Tipos de comunicación 14
Comunicación síncrona y asíncrona 15
Comunicación Serial Síncrona y Asíncrona 16
Protocolos y Servicios 17
Codificación y modulación 18
Corrección y detección de errores 19
Tipos de códigos para detección de errores: 20
Paridad simple (paridad horizontal) 20
Suma de comprobación 20
Hamming (7, 4) 21
Otros códigos para detección de errores: 23
Módems 23
Módem nulo 24
Armado de Módem Nulo 25
Conectando equipos a través de módem nulo 27
Velocidad de transmisión de datos a través del módem nulo: 28
Sumergiéndonos en las redes de computadoras: Conmutación y ruteo 29
Conmutación 29
Conmutación, numeración y ruteo en redes telefónicas: 29
Redes FTTH 30
Modulación AM, FM y QM 31
*Modulación de Amplitud (AM)* 31
*Desventajas* 32
*Utilidad* 33
Algunos cálculos: Ancho de banda y logaritmos 35

Decibelio 35
Ancho de Banda 36
Logaritmos 36
Identidades logarítmicas 37
Relaciones logarítmicas de potencia: 38
Ganancia 39
Ganancia utilizando valores de potencia: 39
Ganancia utilizando valores de voltaje: 39
Ejercicios 40
Capacidad del Canal: 40
Ejercicios 41
Ejercicios para evaluar una primera introducción a las Redes 41
Entrando en la arquitectura de las redes 42
Protocolos, Capas y Servicios 43
El modelo OSI 44
Capas del modelo OSI 45
Capa Física: 45
Capa de Enlace de Datos: 45
Capa de red: 46
Capa de transporte: 46
Capa de Sesión: 46
Capa de Presentación: 46
Capa de Aplicación: 46
El modelo TCP/IP 47
Capas del modelo TCP/IP 49
Capa de Enlace o de Acceso a la Red: 49
Capa de Interred o Internet 49
Capa de Transporte 50
Servicios orientados a Conexión 50
Servicios sin conexión 50
Capa de Aplicación 51
Clasificación de redes según su Topología 51
Red en Anillo 51
Redes en Árbol: 52
Red en Malla: 52

Red en Bus 53
Red en Estrella: 53
Red Celular: 54
Red Mixta: 55
Clasificación de redes según su Alcance 55
Redes de Área Personal (Personal Area Network) 55
Redes de Área Local (Local Area Network) 55
Redes de Área de Campus (CAN) 56
Redes de Área Metropolitana (MAN) 56
Redes de Área Amplia (WAN) 56
Redes de Área de Almacenamiento (SAN) 56
Medios de Red 57
Medios Guiados: Tipos de cable 57
Clasificación de cables par trenzado según blindaje: 58
Clasificación de cables de fibra óptica: 60
Comparativa de velocidad, frecuencia y distancia en medios guiados 60
Ejercicios para evaluar unidad de protocolos y medios de redes 62
Cableado Estructurado 63
Subsistemas del Cableado estructurado 65
Punto de Demarcación (DEMARC) 65
Instalación de entrada (EF) 65
Cableado Dorsal (Backbone) 65
Cuarto de Equipos 66
Gabinete, Armario o Rack de Comunicaciones 66
Cableado Horizontal 66
Área de Trabajo: 66
Cableado Horizontal y Áreas de Trabajo: Consideraciones especiales 67
Oficina Abierta 67
MUTOA (Multiuser Telecommunications Outlet Assembly) 67
Punto de Consolidación (CP) 68
Normas y Códigos para el Cableado - Características Mecánicas 69
Características Eléctricas para el cableado Horizontal 69
Proceso de Instalación del Cableado estructurado (fases) 69
Preventa y Venta 70
Obra Gruesa (Tendido y Ruteo de Cables) 70

Terminación 71
Finalización (Pruebas de Cables y certificación) 71
Asistencia al Cliente 72
Cableado de Enlace Permanente y Enlace de Canal 72
Armado del cableado estructurado 73
Cable Directo 73
Cable Cruzado 74
Procedimiento 74
Uso del Tester de Red 76
Conexión entre equipos 77
Crear una pequeña red local entre dos o varios equipos 78
Creando una red de dos computadoras mediante cable cruzado 78
Configuración de las IP 78
Conectando físicamente los equipos 79
Probando la velocidad de conexión con el comando PING 79
Creando una red de dos o más computadoras utilizando un switch 79
Capa de Enlace 80
Ethernet como tecnología de LAN 81
CSMA/CD 81
Estándar IEEE 802.3 83
Tramas en Ethernet y en 802.3 85
Colisiones y Dominio de Colisiones 86
Funcionamiento de un HUB 87
Funcionamiento de un SWITCH 88
Modos de funcionamiento de un SWITCH 90
Store and Forward 90
Cut-Through 90
Adaptive Cut-Through 90
Configurando un SWITCH Cisco 91
Configuración inicial por consola 92
Comandos genéricos 92
Eliminación de la configuración de la NVRAM 96
Configuración inicial de un Cisco Catalyst 2960 97
Subcapa MAC 101
Codificación Binaria directa 101

Codificación Manchester 102
Codificación Manchester Diferencial 102
Practicando contenidos de la unidad: Visualización de tramas Ethernet y dominios de difusión 103
Uso del software CISCO Packet Tracer 103
Visualización de tramas y paquetes de red 105
Puerta de enlace predeterminada y dirección de Broadcast 108
Capa de Red 110
Protocolos de capa de Red: 110
Protocolo de Internet Versión 4 (IPv4) 110
Protocolo de Internet Versión 6 (IPv6) 111
Redes Privadas 111
Direccionamiento Global y tecnología NAT 111
Direcciones IP públicas 112
Direcciones IP privadas 112
IP Fija o Estática 113
IP Dinámica 113
Traducción de direcciones de red (NAT) 113
***Nat. Estática*** 114
***Dinámica*** 114
Poniendo en práctica algunos contenidos… 114
¿y cómo sé cuál es mi IP pública? 115
Clases de Direcciones IP 116
*Entienda los IP Addresses* 117
Cálculo de clases IP 118
*Máscaras de red* 119
Cálculo de IP dependiendo de requerimientos y Subnetting 120
Subnetting 121
Cálculo de subredes dependiendo de los requerimientos: 122
Ejercicios de ejemplo con subredes de clase C 123
Máscaras de subred con notación barra diagonal 125
Obteniendo direcciones de subred o de host de manera directa 126
Ejercicios de subredes clase A y B 127
A tener en cuenta: 128
Protocolos ARP y RARP 130

Probando el protocolo ARP 131
Servicio DHCP 132
Configurando un servidor DHCP 133
Configurar servicio DHCP en router CISCO 133
Configurando DHCP utilizando un servidor Linux (Ubuntu) 135
Paquetes IP 137
Campos de un paquete IP 138
Práctica visualizando paquetes desde el Packet Tracer 139
Protocolo ICMP 142
Practicando con el comando Traceroute 143
Enrutamiento 144
Funcionamiento de un Router 144
Rutas estáticas y dinámicas 145
Enrutamiento Estático y Dinámico 146
Algoritmos de Enrutamiento 147
Protocolos Enrutados y de Enrutamiento 148
Sistemas Autónomos 149
Practicando contenidos sobre encaminamiento 149
Creación de dos redes LAN independientes con conmutadores CISCO en Packet Tracer 149
Creando redes LAN con switches CISCO usando DHCP 150
Encaminamiento estático con routers CISCO en Packet Tracer 155
Configuración de las tablas de ruteo 160
Capa de Transporte 162
Protocolo de Control de Transmisión (TCP) 163
Segmentos TCP 163
Funcionamiento del protocolo TCP 164
Protocolo de Datagramas de Usuario (UDP) 167
Comparativa con TCP 167
Implementación en lenguajes de programación 168
Capa de Aplicación 169
Funciones de la capa de Aplicación 170
Algunos protocolos de Aplicación 171
DNS: Sistema de Nombres de Dominio 171
Protocolo de Transferencia de Hipertexto (HTTP) 172

Protocolo de Transferencia de Archivos (FTP) 173
Protocolo de Configuración Dinámica del Host (DHCP) 174
Intérprete de Órdenes Seguro (SSH) 174
Actividades prácticas extra 175
Compartir archivos e impresoras en red 175
Compartir recursos en Windows 175
Compartir una impresora en Windows 178
*Compartir la impresora en el PC principal* 178
*Conectar la impresora compartida con el PC secundario* 179
Compartir archivos y carpetas en Linux 180
Utilizando FTP 182
Instalar el servidor FTP en Linux 182
Acceder a un servidor FTP desde un cliente en Linux 183
Accediendo a un equipo remoto por SSH 184
Despedida 186
Bibliografía 187

# Presentación

El propósito de este documento es brindar una guía introductoria sobre redes de computadoras, desde los fundamentos teóricos básicos de comunicación hasta la clasificación de los diferentes tipos de redes y medios. Se brindará una introducción de las diferentes tecnologías de red actuales, como también de su funcionamiento y prestaciones. Se espera transmitir no sólo las nociones básicas, sino también algunos procedimientos necesarios para crear redes domésticas, configurarlas y realizar mantenimiento sobre ellas.

Se menciona el curso de Taller de Mantenimiento II del Plan 2004 del Bachillerato Tecnológico (EMT) de Informática de la Universidad Tecnológica del Uruguay (CETP-UTU) debido a que se buscará cubrir los contenidos del programa de dicho curso, de modo que pueda servir de guía para el estudiante. En la propuesta del curso se busca introducir al estudiante en el mantenimiento Informático en lo que corresponde a redes informáticas, pero involucra la necesidad de utilizar diferentes y extensas fuentes de material, ya que quien escribe es profesor de dicho curso, ha optado por brindar una solución resumida para el estudiante.

Se pretenderá en los temas expuestos, seguir el orden temático de la planificación mencionada, e ir abordando cada tema con una previa exposición de los contenidos

necesarios de saber para su comprensión; no obstante, **no va dirigido únicamente** al **estudiante de la mencionada institución, sino a cualquier lector interesado en el tema.** Es decir, que se invita a leer y utilizarla a todo aquel que esté dando sus primeros pasos en redes, y necesite información resumida.

¡Sin más, saludo cordialmente al lector y comenzamos a trabajar!

## Fundamentos Teóricos Básicos

Antes de analizar cada tema es por ello necesario conceptualizar algunos puntos básicos, como por ejemplo, qué es un medio, qué es una red, cómo se clasifican las redes, qué es una señal y cómo las señales se encuentran clasificadas; debemos precisar también qué entendemos por comunicación y qué tipos de comunicación existen y cuáles son los dispositivos principales que intervienen en una red informática.

Obviaremos para esta etapa, el abordaje de los temas y conceptos relacionados con el hardware y el software (que para el estudiante de UTU, se han trabajado en el curso de Taller de Mantenimiento I), ya que se da por supuesto que el lector de esta guía, ya manejará esa terminología básica; tampoco se requiere para su entendimiento un profundo conocimiento de esos temas anteriores, pero sí se requiere haber comprendido cuáles son los componentes básicos de una PC, qué diferencia hay entre el software y el hardware de una computadora, qué es y cuál es la función de un sistema operativo y qué elementos de la computadora son los requeridos para la instalación y utilización de una red de computadoras.

## Medios

Existen múltiples posibles definiciones de “medio”, dependiendo del área en la cual estemos trabajando y el contexto en el que se utilice la palabra. Incluso limitando su concepto a la informática, tenemos múltiples posibles uso de la palabra, por lo que reduciremos aún más nuestro concepto a lo que corresponde a las redes de computadoras.

Las redes no están creadas para otra cosa que no sea la comunicación, para que exista comunicación entre dispositivos o personas, se requiere de un medio de comunicación, definiremos para esto un medio como *“instrumento o forma de contenido por el cual se realiza el proceso comunicacional o de comunicación. Usualmente se utiliza el término para hacer referencia a los medios de comunicación masivos (MCM, medios de comunicación de masas o mass media); sin embargo, otros medios de comunicación, como el teléfono, no son masivos sino interpersonales” (Wikipedia)*

Sin embargo, cuando estemos hablando de señales por ejemplo, podemos interpretar como el medio al elemento o material sobre el cual se da la comunicación o por donde viajan las señales de comunicación. Por poner un ejemplo práctico, si tenemos dos computadoras conectadas entre sí a través de un cable par trenzado, diremos que el medio por el cual se dan las señales entre ellas será el cable par trenzado (para ese caso particular se requeriría un cable cruzado, pero ya profundizaremos en ese tema).

**En líneas generales, el medio es el canal acordado por el emisor y el receptor, por el cual se transmitirá la información.**

## Red

El concepto de red es muy amplio y tiene aplicaciones en muchas disciplinas independientes de la computación, pero ya cuando escuchamos esa palabra nos podemos imaginar un conjunto de nodos o elementos atados o conectados entre sí. Desde los puntos de intersección de la red de una telaraña, hasta las ataduras de una red de pesca, nos imaginamos partes o áreas del objeto todas interconectadas entre sí. Acercando nuestro concepto a la informática, encontramos el concepto de “red” dentro de las telecomunicaciones (en redes de computadoras o redes telefónicas, por ejemplo), las redes eléctricas, incluso el concepto de red llega tanto a la matemática como a la física en temas que no es el propósito de este documento trabajar.

Para nuestro caso en cuestión, utilizaremos el concepto de **redes de computadoras,** y el mejor ejemplo que se ha encontrado para este trabajo, es el concepto que plantea Tanembaum donde afirma que *“(…) utilizaremos el término “red de computadoras” para referirnos a un conjunto de computadoras autónomas interconectadas mediante una sola tecnología. Se dice que dos computadoras están interconectadas si pueden intercambiar información. La conexión no necesita ser a través de un cable de cobre; también se puede utilizar fibra óptica, microondas, infrarrojos y satélites de comunicaciones. Las redes pueden ser de muchos tamaños, figuras y formas, como veremos más adelante. Por lo general se conectan entre sí para formar redes más grandes, en donde* ***Internet*** *es el ejemplo más popular de una red de redes.”* (Tanembaum, 2014).

Como vemos en este concepto, ya se mencionan medios para interconectar computadoras, en este caso se menciona el cable de cobre, la fibra óptica, las microondas, infrarrojos y satélites de comunicaciones. Todos éstos, son medios para la comunicación en red. Menciona el concepto de Internet como un conjunto de redes (que además pueden ser de muy diversos tamaños). Cuando hablamos de computadoras, también debemos quitarnos el preconcepto de que es una PC con su respectivo monitor, teclado y ratón, sino que con la expansión de la tecnología y en particular la tecnología móvil, debemos saber que en nuestro bolsillo llevamos una poderosa computadora portátil que es nuestro teléfono celular, y que dicha computadora está conectada a redes de varios tipos a su vez (está conectado a Internet pero suele estar conectado también por satélites GPS, así como a la misma red celular e incluso una red de área personal si lo estamos utilizando con auriculares u otros dispositivos conectados).

La clasificación de las redes de computadoras, puede ser diferente dependiendo del criterio que utilicemos (por alcance, tipo de conexión, tecnología, topología, etc). Más adelante se irán trabajando las clasificaciones fundamentales por separado.

## Señal

Definiremos a una señal como *"un gesto u otro tipo de informe o aviso de algo. La señal sustituye por lo tanto a la palabra escrita o al lenguaje. Ellas obedecen a convenciones, por lo que son fácilmente interpretadas. (…) Asimismo, una señal puede ser también la variación de una u otra magnitud física que se utiliza para transmitir información. Por ejemplo, en telefonía existen diferentes señales, que consisten en un tono continuo o intermitente, en una frecuencia característica, que permite conocer al usuario en qué situación se encuentra la llamada."* (Wikipedia)

Para nuestro trabajo, el concepto de señal que manejaremos será el que corresponda a la corriente eléctrica o una magnitud física que permite transmitir información. Digamos que las computadoras entre sí, así como dentro de las computadoras existe un alto grado de comunicación entre componentes, ésta comunicación se da a velocidades extremadamente altas, y consiste en pulsos eléctricos que son interpretados por los diferentes componentes de la máquina.

Para comprender esto, debemos recordar que el lenguaje de máquina es binario, ¿No encontramos alguna relación entre el lenguaje de los 0s y los 1s con el hecho de que un instante determinado fluya o no corriente eléctrica por un cable? Esos pulsos eléctricos, son las señales que permiten que exista comunicación entre diferentes máquinas.

Las señales que estudiaremos pueden clasificarse en dos tipos fundamentales:

**Señal Analógica:** Es emitida generalmente por un fenómeno electromagnético y representada por una función matemática continua que puede variar en su amplitud y su período, en concreto, una característica de ellas es que se representan con medidas físicas, y son comúnmente usadas para la transmisión de video o sonido. En su aplicación tecnológica, como en la transmisión multimedia, para que estas señales sean interpretadas es requerido un decodificador que cumpla con ese trabajo; sin embargo, en

la naturaleza podemos percibir algunas señales, todas ellas analógicas, como ser la luz o el sonido.

**Señal Digital:** Las señales digitales son en esencia señales continuas, pero interpretadas de un modo diferente, no se interpretan según un rango de valores sino que se llevan a unidades discretas, es decir, se interpretan por ejemplo según posibles estados de la señal. Por ejemplo, una señal alta o una señal baja en un muy corto período de tiempo, lo que denominamos como un instante.

Dentro de una computadora por ejemplo, existen dispositivos que se comunican entre sí mediante señales digitales que se interpretan según dos posibles estados utilizando para ello lógica binaria. Nuevamente tomamos un concepto previamente analizado de Wikipedia, donde nos dice que *"La señal digital es un tipo de señal en que cada signo que codifica el contenido de la misma puede ser analizado en término de algunas magnitudes que representan valores discretos, en lugar de valores dentro de un cierto rango. Por ejemplo, el interruptor de la luz sólo puede tomar dos valores o estados: abierto o cerrado, o la misma lámpara: encendida o apagada (véase circuito de conmutación). Esto no significa que la señal físicamente sea discreta ya que los campos electromagnéticos no suelen ser continuos, sino que en general existe una forma de discretizarla unívocamente.*

*Los sistemas digitales, como por ejemplo el ordenador, usan la lógica de dos estados representados por dos niveles de tensión eléctrica, uno alto, H y otro bajo, L (de High y Low, respectivamente, en inglés). Por abstracción, dichos estados se sustituyen por ceros y unos, lo que facilita la aplicación de la lógica y la aritmética binaria. Si el nivel alto se representa por 1 y el bajo por 0, se habla de lógica positiva y en caso contrario de lógica negativa."*(Wikipedia)

Como podremos imaginar, para su aplicación en redes informáticas, las señales digitales ofrecen mayor flexibilidad y fidelidad, ya que los datos no se deterioran ni se pierden con tanta facilidad como en las analógicas, ya que gracias a determinados algoritmos, se pueden detectar e incluso corregir errores en la comunicación.

Recordemos que hace unos años, la señal de cable de TV por ejemplo era analógica, y cuando más recientemente las compañías de cable fueron innovando en tecnologías digitales, se hacían publicidad de ello ya que los canales de TV se comenzaron a transmitir en mejor definición, además de que las canaleras (pequeñas computadoras conectadas a la red de TV por cable coaxial) comenzaron a portar pequeños softwares que permiten elegir canales de manera más sencilla, incluso ver qué programas se están transmitiendo en cada canal o hasta saber qué programación tendrán en el transcurso del día. Todo ello no era posible con la señal analógica.

## Comunicación

Adentrándonos ya en el campo de las redes de computadoras, hay un concepto fundamental que hemos mencionado y hemos pasado por alto de conceptualizar, tal vez porque lo damos por conocido, y es que de hecho ya resulta familiar a todos, pero el concepto de comunicación en lo que refiere a redes no sólo es fundamental, sino que detallarlo nos servirá para comprender futuros conceptos. Nuestro diccionario maneja varias posibles definiciones, la que más se adapta a nuestra área, es la siguiente: *"Transmisión de señales mediante un código común al emisor y al receptor."* (RAE) .

Así de sencillo, sin embargo, notemos que aquí se menciona la necesidad de que exista un código común entre el emisor y el receptor de cada señal, esto es, un lenguaje común en el que ambos se puedan entender. Parece obvio, imaginar que exista comunicación fluida verbal entre una persona que sólo habla español y otra que únicamente habla ruso, ¿verdad? Necesitamos de un **código** o una serie de acuerdos comunes que permitan que ambas partes se entiendan, por ejemplo, entre personas un idioma que ambos dominen.

En redes de computadoras, veremos más adelante que esta necesidad se asocia con la existencia de diferentes protocolos de comunicación, que permiten que diferentes elementos puedan comunicarse entre sí.

## Dispositivos DCE y DTE

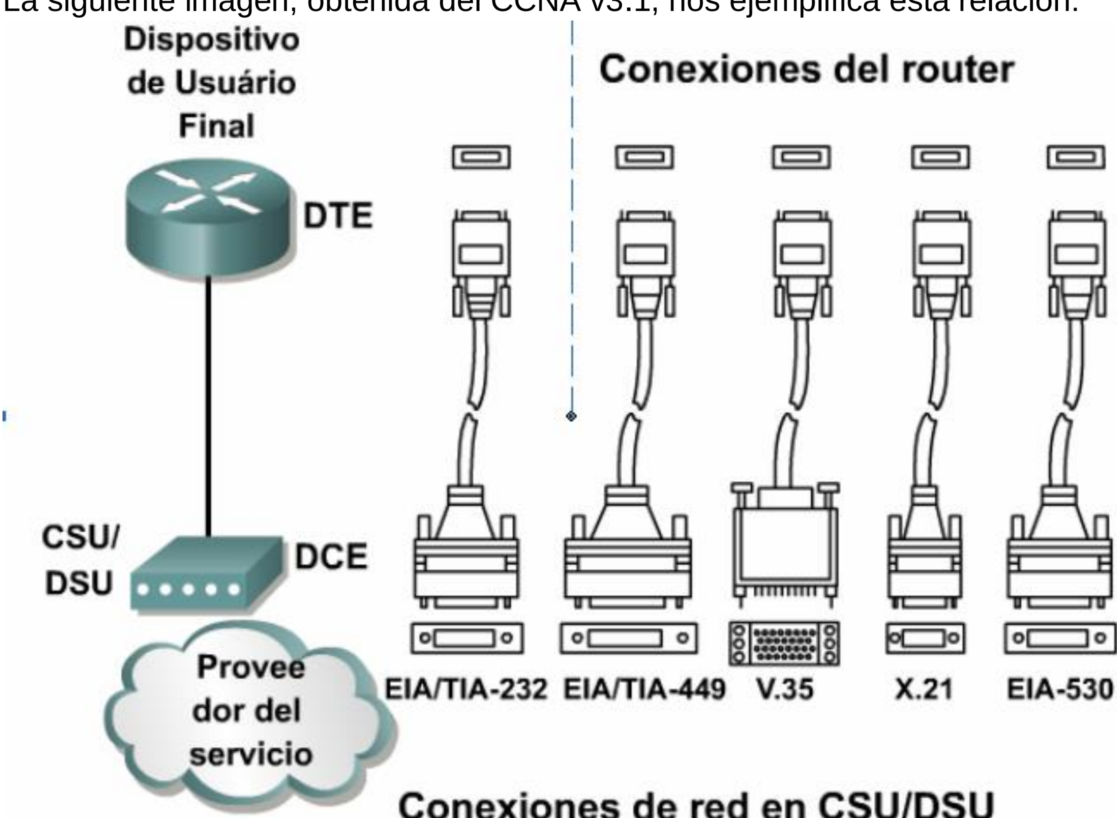
Imaginemos la red de computadoras que casi todos usamos a diario, Internet, ésta red es en realidad una interred, un enorme conjunto de redes de diversas dimensiones conectados entre sí, existen entre ellas, un enorme conjunto de dispositivos estableciendo comunicación entre sí. Para dar una breve clasificación, diremos que algunos de ellos son proveedores de servicios de comunicación (DCE) y otros son terminales o dispositivos conectados (DTE).

- Un Equipo de Terminación del Circuito de Datos o de Comunicación de Datos (DCE) es aquel que se encarga de proveer datos, es por ejemplo un modem, que se encarga de proveer conexión.
- Un Equipo Terminal de Datos (DTE) son los dispositivos conectados a la red, que se encargan de recibir los datos, por ejemplo una computadora, una impresora o un puente, pueden funcionar como terminales de datos.

Los routers por ejemplo, son dispositivos muy importantes en la instalación de redes, y dependiendo de la función para la cual se encuentren instalados, pueden funcionar como DCE o como DTE, tengamos en cuenta la siguiente aclaración:

*“Si la conexión se hace directamente con el proveedor de servicio, o con un dispositivo que provee señal de temporización tal como la unidad de servicio de canal/datos (CSU/DSU), el router será un equipo terminal de datos (DTE) y usará cable serial DTE. Por lo general, este es el caso. Sin embargo, hay situaciones en las que se requiere que el router local brinde la temporización y entonces utilizará un cable para equipo de comunicación de datos (DCE). En las prácticas de laboratorio incluidas en el currículo, uno de los routers conectados necesitará brindar la función de temporización. Por lo tanto, la conexión estará formada por un cable DCE y DTE.”* (CCNA)

La siguiente imagen, obtenida del CCNA v3.1, nos ejemplifica esta relación:




## Tipos de comunicación

La comunicación entre dispositivos informáticos puede darse de diferentes maneras, la clasificación fundamental proviene de la electrónica y se trata de diferenciar comunicación serial de comunicación paralela. El concepto en sí, es el mismo que se maneja con la electricidad, con la diferencia de que, en lugar de estar hablando de corriente eléctrica, estamos hablando de flujo de datos (los que a su vez requieren corriente eléctrica por supuesto).

Cuando existe comunicación de datos, hay transmisión de bits de datos, esto es, transmisión de señales digitales en sus 2 posibles estados.

**En la comunicación en serie** los datos que envía el emisor al receptor viajan 1 bit a la vez (en el lenguaje coloquial, viajan uno detrás de otro), lo hace de manera secuencial, mientras que **la comunicación en paralelo** implica que se envían varios bits a la vez, siendo ésta una comunicación simultánea permitiendo a priori, mayores cantidades de datos.

Ambos tipos de comunicación son utilizados en la actualidad, pero dependiendo del fin que se tenga, puede haber ventajas en un tipo frente a otro. Ya dijimos que en la comunicación en paralelo viajan varios datos a la vez, con lo cual apresuradamente cualquiera podría decirnos que es mejor, que permite transmitir más datos, pero sin embargo, las interfaces de comunicación más modernas que se utilizan en las computadoras actuales, suelen ser seriales, y se está dejando atrás el uso de comunicación paralela por ejemplo para conectar dispositivos de almacenamiento o

periféricos, la interfaz USB es uno de los estándares actuales y está mejorando cada vez, pudiendo ofrecer velocidades cada vez mayores de transferencia de archivos. ¿Por qué ocurre esto?

- La comunicación en serie utiliza lógicamente menos cables, lo que la hace más segura para llevar datos a largas distancias, además, evita que los datos se distorsionen ya que con la comunicación paralela, puede existir interferencia entre los diferentes cables.
- Los puertos seriales requieren menos pines que los paralelos (ya que conectan con menos alambres) por lo que son de menor tamaño, optimizando así el espacio y reduciendo el costo.

En las redes, así como en el armado de dispositivos de hardware, existen ambos sistemas de transmisión, y dependiendo del caso se utiliza uno u otro, familiarizarse con cada concepto, es una necesidad esencial para el desarrollo de este trabajo.

## Comunicación síncrona y asíncrona

Además del modo en el cual fluyen los datos, la comunicación se puede clasificar según su relación entre emisor y receptor. Imaginemos a dos amigos charlando en una esquina planificando hacer una comida juntos el fin de semana. Cuando un amigo habla es emisor, mientras que quien lo escucha es receptor, pero cuando el receptor contesta y por ejemplo, expone otras razones y dice su opinión, se convierte en el nuevo emisor del mensaje mientras que el que antes emitió un mensaje, pasa a quedar como receptor. Los roles cambian y así en la conversación van variando, en este caso están realizando una conversación en tiempo real, en vivo y en directo, y diremos que es síncrona o sincrónica.

Sin embargo, la comunicación puede ser de otros tipos, incluso en las redes de computadoras, puede existir comunicación sincróna y también asíncrona.

- La comunicación sincrónica (síncrona) es la que se da en tiempo real, por ejemplo en el caso de una llamada telefónica, donde los dos pares se encuentran compartiendo un mismo canal de comunicación y se encuentran conversando casi a la misma velocidad que si lo hicieran personalmente.
- La comunicación asincrónica (asíncrona), por su parte, es la que ocurre de manera diferida en el tiempo, por ejemplo en la Mensajería de Textos Cortos (SMS), en los mensajes de correo electrónico, o fuera del ámbito de las redes informáticas, en una carta escrita en papel.

En toda comunicación, intervienen varios elementos:

➢ Emisor: El emisor envía la información sabiendo que no obtendrá una respuesta inmediata.

➢ Receptor: Este será consciente de la llegada del mensaje solo cuando acceda al canal específico.

➢ Canal: Es el medio físico acordado por ambas partes por el que se transmite el mensaje, debe ser perdurable en el tiempo ya que el mensaje se almacenará allí durante un tiempo indefinido.

- ➢ Código: Debe ser perdurable en el tiempo, además deberá ser compartido entre los elementos del evento comunicativo; deberá contar con un soporte físico para su almacenamiento.

- ➢ Situación o contexto: La disponibilidad del emisor o receptor es incierta y marca de forma importante el contexto de la comunicación.

## Comunicación Serial Síncrona y Asíncrona

Una vez que ya hemos trabajado un concepto de comunicación, y que se ha definido y diferenciado la comunicación en serie de la comunicación en paralelo; cabe preguntarnos qué tiene que ver ésta clasificación con los medios de comunicación sincrónica y asincrónica que se definieron anteriormente. Sucede que, en las redes de computadoras podemos encontrar tecnologías de comunicación en serie, que a su vez pueda o no tener una sincronía en relación al tiempo. ¿Cómo funciona ésto? Bien, primero que nada cuando hablamos de sincronía o asincronía tenemos que tener en cuenta un factor determinante: el tiempo. Si pregunto, ¿Cómo se mide el tiempo? Usted lector, pensará, ¡Qué pregunta elemental!, ¡Con un reloj! Entonces ambos tipos de comunicación se diferencian precisamente en eso, en que en los sistemas en serie asíncronos no se usa ningún cable para enviar pulsos de reloj, mientras que sí se hace en los síncronos. Conceptualizando:

- En la comunicación Serial Asíncrona se utiliza un cable compuesto por los siguientes hilos: 1 para alimentación (llamado VCC), 1 para tierra (llamado GND), y 1 para datos. Sólo 3 hilos de cable componen un cable para establecer comunicación serial síncrona. Los datos viajarán bit a bit a través del hilo de datos, pero, para que efectivamente pueda existir comunicación entre emisor (Tx) y receptor (Rx) es necesario que ambos se pongan de acuerdo en los siguientes parámetros, es decir, hay que establecer los siguientes “protocolos”:

  - ➢ La velocidad de transmisión tiene que ser la misma en ambos dispositivos (Tx y Rx), expresada en baudios (bits/s)
  - ➢ Ambos deben definir la cantidad de bits a enviar o recibir para cada paquete.
  - ➢ La paridad que se va a utilizar (ver capítulo de detección y corrección de errores)
  - ➢ Cuantos bits de parada (para separar caracteres) se van a recibir.

  Si no existe acuerdo en los parámetros anteriores, no puede existir comunicación, recordar el viejo dicho “cuando un burro habla, el otro se calla”.

- La comunicación serial síncrona, tiene además del VCC, el cable de datos y el GND, un cable adicional, que es el que transmitirá los pulsos del reloj. Como la comunicación se va a dar respetando dichos pulsos, las “palabras” serán separadas de acuerdo a ellos y no será necesario que el emisor y el receptor “hablen” a la misma velocidad, sino que podrán funcionar con velocidades de transferencia diferentes.

## Protocolos y Servicios

A lo largo de este trabajo mencionaremos normalmente el concepto de protocolo, ya que es un concepto bien importante en lo que corresponde a redes, retomando lo que se decía anteriormente sobre el concepto de comunicación, decíamos que la comunicación era la *“transmisión de señales mediante un código común entre el emisor y el receptor”*, entonces podemos decir que los protocolos son ese código común entre los pares de comunicación.

Un protocolo es una convención de reglas a seguir para hacer posible la comunicación entre dos partes, para que esas partes puedan entenderse. En redes, existe una clasificación común que detallaremos más adelante que corresponde a la arquitectura de una red, en la cual se estudia una red según diferentes clases o niveles de abstracción, a los que se les denomina capas, y existen protocolos de comunicación diferentes para cada capa, es decir, para cada nivel de abstracción en la arquitectura de una red.

Los servicios por su parte son funciones que permiten la comunicación entre esos diferentes niveles, son interfaces que permiten que los mensajes puedan ser armados para su transmisión de una capa inferior a una superior y viceversa; pero no nos quedemos con las palabras de la humilde persona quien escribe, veamos qué dice Tanembaum al respecto:

*“Los servicios y los protocolos son conceptos distintos. Esta distinción es tan importante que la enfatizaremos una vez más. Un servicio es un conjunto de primitivas (operaciones) que una capa proporciona a la capa que está encima de ella. El servicio define qué operaciones puede realizar la capa en beneficio de sus usuarios, pero no dice nada sobre cómo se implementan estas operaciones. Un servicio se relaciona con una interfaz entre dos capas, en donde la capa inferior es el proveedor del servicio y la capa superior es el usuario.*
*En contraste, un protocolo es un conjunto de reglas que rigen el formato y el significado de los paquetes o mensajes que intercambian las entidades iguales en una capa. Las entidades utilizan protocolos para implementar sus definiciones de servicios. Pueden cambiar sus protocolos a voluntad, siempre y cuando no cambien el servicio visible para sus usuarios. De esta manera, el servicio y el protocolo no dependen uno del otro. Éste es un concepto clave que cualquier diseñador de red debe comprender bien. Para repetir este punto importante, los servicios se relacionan con las interfaces entre capas, como se muestra en la figura 1-19. En contraste, los protocolos se relacionan con los paquetes que se envían entre las entidades pares de distintas máquinas. Es muy importante no confundir los dos conceptos.”*

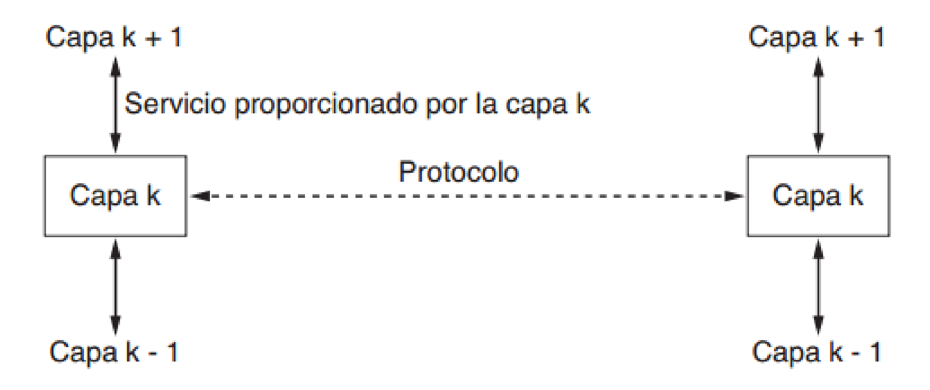



**Figura 1-19.** La relación entre un servicio y un protocolo.

(Tanembaum, 2014)

## Codificación y modulación

Cuando se habla de codificación, el concepto puede también tener multiplicidad de interpretaciones, sin embargo debemos acotar todos los conceptos a nuestro ámbito concreto. Siendo que queremos conceptualizar, volveremos a citar luego de su análisis, a Wikipedia.

Codificación: *"Se entiende por **codificación** en el contexto de la Ingeniería, al proceso de conversión de un sistema de datos de origen a otro sistema de datos de destino. De ello se desprende como corolario que la información contenida en esos datos resultantes deberá ser equivalente a la información de origen. Un modo sencillo de entender el concepto es aplicar el paradigma de la traducción entre idiomas en el ejemplo siguiente: home = hogar. Podemos entender que hemos cambiado una información de un sistema (inglés) a otro sistema (español), y que esencialmente la información sigue siendo la misma. (…) En ese contexto la codificación digital consiste en la traducción de los valores de tensión eléctrica analógicos que ya han sido cuantificados (ponderados) al sistema binario, mediante códigos preestablecidos. La señal analógica va a quedar transformada en un tren de impulsos de señal digital (sucesión de ceros y unos). Esta traducción es el último de los procesos que tiene lugar durante la conversión analógica-digital. El resultado es un sistema binario que está basado en el álgebra de Boole." (Wikipedia)*

Ahora bien, para seguir entendiendo estos conceptos según el hilo conductor que estamos teniendo, debemos entrar en otro concepto, y es en el de **onda portadora.** Sabemos como se ha esbozado antes, que cuando hablamos de señales análogas o digitales estamos hablando de señales cuyas magnitudes pueden representarse en forma de gráfico, generalmente de tipo sinusodial (este concepto deriva de las matemáticas, y quiere decir que se representan gráficamente mediante la curva de la función seno).

Onda portadora: Las ondas portadoras son ondas de radio, generalmente de tipo sinusoide que han sido modificadas para enviar información, aunque una onda sin modificar también se puede llamar portadora. Las modificaciones pueden ocurrir de varias

maneras como con los conocidos métodos de AM y FM usadas en las radios. Es posible propagar esto como ondas electromagnéticas o ser transmitidas por medios físicos.

Modulación: *"engloba el conjunto de técnicas que se usan para transportar información sobre una onda portadora, típicamente una onda sinusoidal. Estas técnicas permiten un mejor aprovechamiento del canal de comunicación lo que posibilita transmitir más información de forma simultánea además de mejorar la resistencia contra posibles ruidos e interferencias. Según la American National Standard for Telecommunications, la* ***modulación*** *es el proceso, o el resultado del proceso, de variar una característica de una onda portadora de acuerdo con una señal que transporta información. El propósito de la modulación es sobreponer señales en las ondas portadoras.*[1]

*Básicamente, la modulación consiste en hacer que un parámetro de la onda portadora cambie de valor de acuerdo con las variaciones de la* ***señal moduladora****, que es la información que queremos transmitir.." (Wikipedia)*

## Corrección y detección de errores

Cuando hablamos de comunicación por medio de señales analógicas, muchas veces sucede que la información se pierde o se distorsiona, esto para algunos casos no es demasiado importante en niveles aceptables, por ejemplo, en una llamada telefónica donde es imprescindible que ambas partes se entiendan, sin embargo, se puede aceptar que a veces el mensaje pueda sufrir alguna distorsión, siempre que se entienda. Ahora bien, para medios más específicos, donde se utiliza comunicación digital, por ejemplo si estamos realizando una comunicación de datos entre dos bancos a través de la red, esto es inaceptable, en particular con datos confidenciales, se pretende que la información llegue, pueda ser almacenada y que sobre todo no se pierda.

Si un usuario se conecta a Internet para realizar cualquier operación financiera, así como para hablar con sus amigos, es necesario también que ese mensaje llegue íntegro, ya que cuando estamos enviando señales digitales, cualquier ruido que afecte al mensaje que se envía y que produzca pérdida de bits, puede ser interpretado de forma completamente distinta.

Los módems, dispositivos a los que vamos a abordar en breves líneas, son en esencia digitalizadores y moduladores de información, permiten una conexión a Internet usando la línea telefónica, se encargan de digitalizar las señales analógicas de la red telefónica para que el computador las interprete, ya su vez modulariza los datos digitales que el computador envíe para ser transmitidos por la señal telefónica. Este proceso es susceptible a errores en ambos procedimientos, y para evitar pérdida o corrupción de la información, los diferentes módems utilizan sistemas para la detección y corrección de esos eventuales errores.

*La comunicación entre varias computadoras produce continuamente un movimiento de datos, generalmente por canales no diseñados para este propósito (línea telefónica), y que introducen un ruido externo que produce errores en la transmisión.*

*Por lo tanto, debemos asegurarnos que si dicho movimiento causa errores, éstos puedan ser detectados. El método para detectar y corregir errores es incluir en los bloques de datos transmitidos bits adicionales denominados redundancia.*

*Se han desarrollado dos estrategias básicas para manejar los errores:*

- *Incluir suficiente información redundante en cada bloque de datos para que se puedan detectar y corregir los bits erróneos. Se utilizan **códigos de corrección de errores**.*
- *Incluir sólo la información redundante necesaria en cada bloque de datos para detectar los errores. En este caso el número de bits de redundancia es menor. Se utilizan **códigos de detección de errores**.*

*Si consideramos un bloque de datos formado por **m** bits de datos y **r** de redundancia, la longitud final del bloque será **n**, donde **n** = **m** + **r**.*

(Wikipedia)

## Tipos de códigos para detección de errores:

### Paridad simple (paridad horizontal)

Consiste en añadir un bit de más a la cadena que queremos enviar, y que nos indicará si el número de *unos* (bits puestos a 1) es par o es impar. Si es par incluiremos este bit con el valor = 0, y si no es así, lo incluiremos con valor = 1.

Ejemplo de generación de un bit de paridad simple:

*Queremos enviar la cadena "1110100":*
*1º Contamos la cantidad de unos que hay: 4 unos*
*2º El número de unos es par por tanto añadimos un bit con valor = 0*
*3º La cadena enviada es 11101000*

El receptor ahora, repite la operación de contar la cantidad de "unos" que hay (menos el último bit) y si coincide, es que no ha habido error.

**Problemas de este método:**

Hay una alta probabilidad de que se *cuelen* casos en los que ha habido error, y que el error no sea detectado, como ocurre si se cambian dos números en la transmisión en vez de uno.

### Suma de comprobación

Es un método sencillo pero eficiente sólo con cadenas de palabras de una longitud pequeña, es por esto que se suele utilizar en  de tramas importantes u otras cadenas importantes y en combinación con otros métodos.

Funcionalidad: consiste en agrupar el mensaje a transmitir en cadenas de una longitud determinada L no muy grande, de por ejemplo 16 bits. Considerando a cada cadena como un número entero numerado según el sistema de numeración . A continuación se suma el

valor de todas las palabras en las que se divide el mensaje, y se añade el resultado al mensaje a transmitir, pero cambiado de signo.

Con esto, el receptor lo único que tiene que hacer es sumar todas las cadenas, y si el resultado es 0 no hay errores.

Ejemplo:

Mensaje 101001110101

1º Acordar la longitud de cada cadena: 3

2º Acordar el sistema de numeración:

3º Dividir el mensaje: 101 001 110 101

4º Asociar cada cadena con un entero: 5 1 6 5

5º Sumar todos los valores y añadir el número cambiado de signo: -17

6º Enviar 5 1 6 5 -17 codificado en
El receptor:

1º Suma todos los valores; si la suma es 0, procesa el mensaje; si no, se ha producido un error.

## Hamming (7, 4)

El matemático Richard Hamming desarrolló en la década de los años 1940s y 1950s códigos para detección de errores en señales de comunicación binaria. El 7, 4 es uno de los algoritmos más conocidos, también llamado coloquialmente como "Código Hamming".

Consiste en tomar palabras de 7bits de datos, a los que se le añade una redundancia de 4 bits denominados de "paridad". Los bits de paridad le servirán al algoritmo para lograr los dos objetivos más importantes:

- Detectar errores en una palabra recibida
- Corregir los errores detectados

El algoritmo sirve para detectar errores en un bit de la palabra y reconstruirla, para dos o más bits, se usa una variación del algoritmo que se le llama Hamming Extendido (Wikipedia).

El procedimiento es el siguiente:

4. Dejamos 4 filas debajo para bajar o “descomponer” la palabra, según corresponda:

En la primer fila bajamos los bits de la palabra original comenzando desde la posición del primer bit de paridad y salteando de a 1 bit.

En la segunda fila bajamos los bits de la palabra original comenzando desde la posición del segundo bit de paridad y salteamos de a 2 bits.

En la tercera fila bajamos los bits de la palabra original comenzando desde la posición del tercer bit de paridad y salteando de a 4 bits.

En la cuarta fila bajamos los bits de la palabra original comenzando desde la posición del cuarto bit de paridad y salteando de a 8 bits.

5. Luego para cada fila verificamos la cantidad de 1s, si es par o impar, y nos reservamos una columna al lado para indicar con un 1 si es impar, y con un 0 si es par.
6. En cada fila donde la paridad resultante sea 1, indica que tenemos un error, y debemos buscar en las columnas de los bits que bajamos, en cual podemos cambiar un bit de la palabra original, para que la paridad resultante sea par en todas las filas.
7. Encontrada dicha columna, cambiamos el bit correspondiente y así el error estará reparado.

Ejemplo:

Palabra recibida: 0110101

- Colocamos la palabra en la tabla correspondiente y reservamos los espacios “P” para bits de paridad, “D” para bits de datos y una columna extra para la paridad de cada fila: ***Importante: En los espacios donde bajamos un bit de paridad, inicialmente colocamos 0 (bajamos un 0 en las columnas de paridad)***

| **Bits:** | P1 | P2 | D1 | P3 | D2 | D3 | D4 | P4 | D5 | D6 | D7 | **Paridad** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **0** | | **1** | **1** | **0** | | **1** | **0** | **1** | |
| **P1** | **1( era un 0. Al final del ejercicio, lo cambiamos)** | | 0 | | 1 | | 0 | | 1 | | 1 | 1 (Pasa a 0 al cambiar P1) |
| **P2** | | 0 | 0 | | | 1 | 0 | | | 0 | 1 | 0 |
| **P3** | | | | 0 | 1 | 1 | 0 | | | | | 0 |
| **P4** | | | | | | | | 0 | 1 | 0 | 1 | 0 |
| → | ***1*** | ***0*** | ***0*** | ***0*** | ***1*** | ***1*** | ***0*** | ***0*** | ***1*** | ***0*** | ***1*** | |

- Luego de bajar los valores correspondientes en la posición correspondiente, contamos la paridad de cada fila. (Recordar, colocamos 0 en paridad par, 1 en paridad impar).

- En el ejemplo vemos 1 fila con error, por lo cual debemos detectar y modificar el bit de la palabra, que genera que que dicha fila tenga paridad impar, y así corregir el error. Si hubiesen más filas con errores, entonces debemos buscar el bit que genere imparidad en dichas filas y no en las que han llegado correctamente.
- **Nótese que para que la palabra no genere imparidad debemos modificar la primer columna, es decir, el primer bit de paridad.**
- ***La palabra con el error corregido, nos queda como resultado 10001100101***

## Otros códigos para detección de errores:

- Distancia Mínima de Hamming
- Dígito verificador
- Código Binario de Golay
- Código de Redundancia Cíclica (CRC)

## Módems

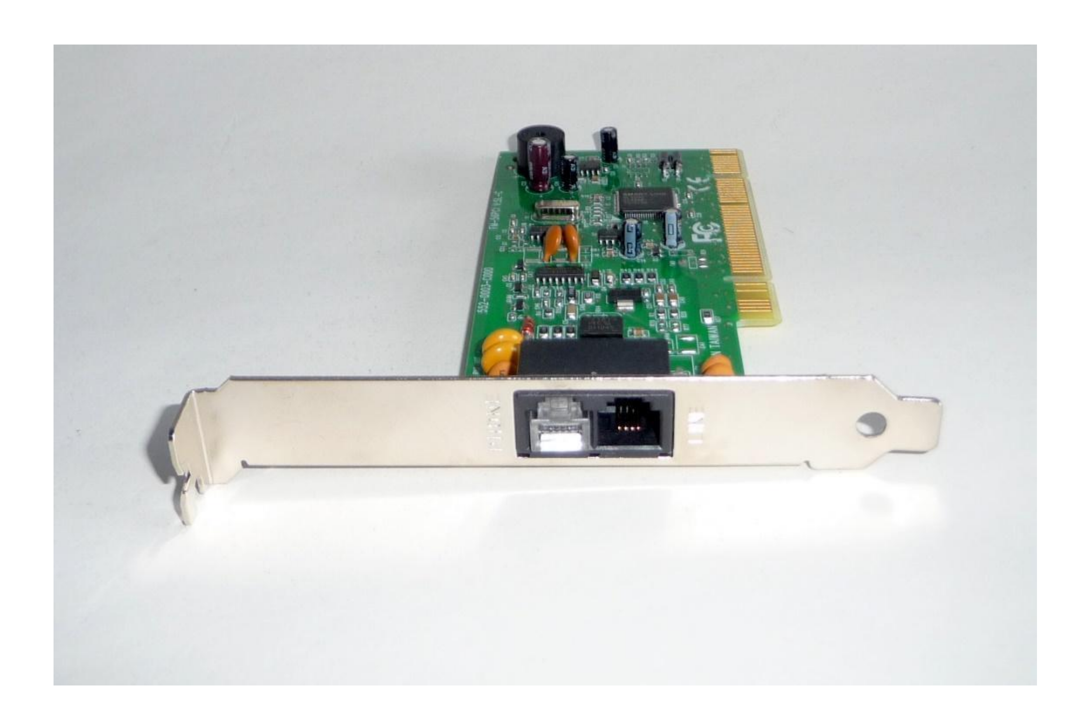
Podemos decir que un módem es un dispositivo que convierte señales digitales en analógicas, o viceversa, para poder ser transmitidas a través de líneas de teléfono, cables coaxiales, fibras ópticas y microondas; conectado a una computadora, permite la comunicación con otra computadora por vía telefónica.

Existen módems internos, que se instalan dentro del PC en la placa base y otros externos, que se conectan a la computadora a través de algún puerto.

Actualmente conocemos como módems a dispositivos capaces de conectarse con la red celular a través de tecnologías 3G (que permiten comunicación por voz y datos digitales) con el fin de permitirnos acceso a Internet en cualquier sitio con cobertura de datos móviles con conexión WCDMA, HSDPA o LTE a velocidades decentes, de hecho por ejemplo la conexión LTE (conocida como 4G LTE) permite velocidades de conexión altas, de hasta 25 Mbps. No obstante, si nos remontamos al concepto original de módem, que modulaban a través de señales analógicas FSK, PSK, QAM a través de la línea telefónica, las velocidades eran inimaginablemente inferiores.

Para hablar de datos concretos y no tan antiguos, los módems de modulación digital de los más actuales, a principios de los 2000, permitían una velocidad de conexión de hasta 56 Kbps de descarga. En la actualidad, una conexión móvil LTE ofrece velocidades de más de 400 veces más altas, ¡y toda esta evolución tuvo lugar en apenas unos 15 años!

En la imagen a continuación, podemos ver un módem interno que se conectaba a la computadora a través del bus PCI y ofrecía una velocidad de 56 Kbps:



## Módem nulo

Este es el nombre que se le asigna a un método para conectar dos terminales usando un cable serie .

En la confección del módem nulo las líneas de transmisión y recepción están cruzadas. Existe más de una forma de realizar una conexión módem nulo ya que no hay ningún estándar que defina esta conexión. En cualquier caso, se utiliza un cable de tipo serial conectado en cada extremo al puerto serial de cada equipo.

*Estos cables son comúnmente usados para la transferencia de archivos. En el sistema operativo Microsoft Windows la conexión directa por cable se puede realizar con un cable módem nulo. Las últimas versiones de MS-DOS traían el programa Interlink. El mismo permitía trabajar con el disco duro de la computadora remota como un disco de red. Hay que aclarar que no se necesitaba ningún hardware adicional como una placa de red, la conexión se podía realizar fácilmente con un cable módem nulo. (Wikipedia)*

En la imagen siguiente, podemos ver un cable de conexión serial RS 232:



## Armado de Módem Nulo

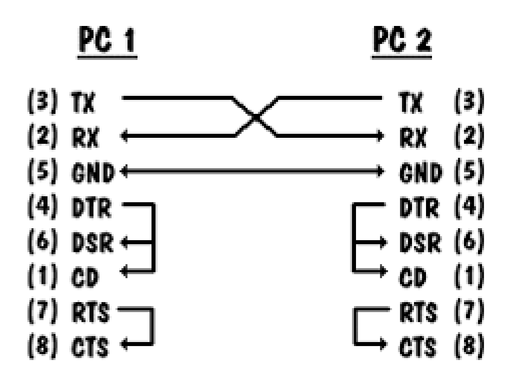
El cable módem nulo consiste en un cable para la comunicación serial entre 2 PCs, con una ficha hembra DB9 en cada uno de sus extremos. Su armado no tiene una lógica complicada pero sí requiere de algo de tiempo y paciencia. A continuación se detallarán los materiales necesarios, y posteriormente el proceso para realizar el armado.

Herramientas necesarias:

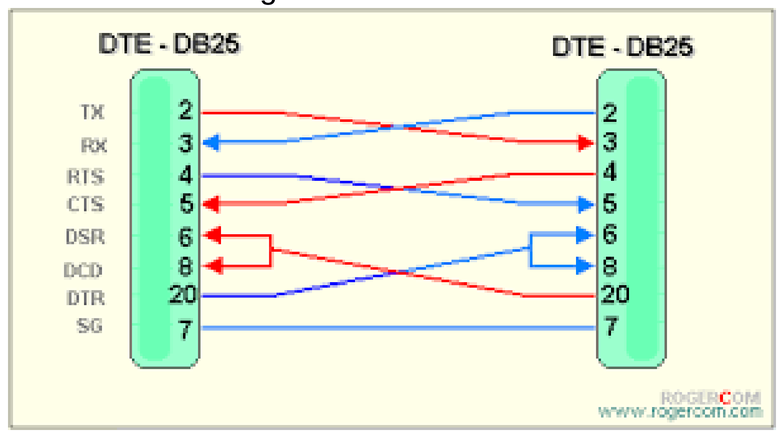
- 2 conectores DB-9 hembras
- 2 cajas para DB-9
- Cable par trenzado (UTP) de **menos** de 30 metros de largo
- Pinza para pelar cables.
- Navaja o alicate
- Soldadora de estaño y estaño
- Destornillador.
- Pistola de silicona o silicona líquida (recomendado)

Procedimiento:

1) El primer paso es tomar el cable UTP de 8 hilos y pelar aproximadamente unos 3cm en cada extremo del cable.
2) Desenredar los cables trenzados que aparecerán dentro del UTP y pelarlos cuidadosamente a unos 3mm cada uno.
3) Estañar cada uno de los extremos de los cables desenrollados cuidadosamente para luego soldar al conector DB-9.
4) Respecto al orden de los colores de los cables que soldaremos en cada extremo (tema que inmediatamente estaremos trabajando) cabe destacar que en el esquema del cable RS-232 será el siguiente (en caso de estar armando un modem nulo con conectores DB-9):




Si en lugar de usar conectores DB-9, usáramos el otro estándar de cables de serie, el DB-25 (claramente identificable por ser mucho más ancho), la conexión a realizar sería la siguiente:




*(Imágenes obtenidas del blog: Telemática).*

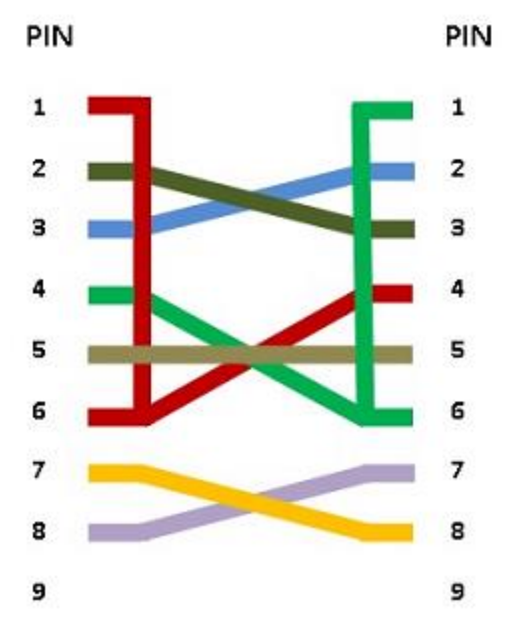
Continuamos con el procedimiento, soldado los cables trenzados del siguiente modo:

A. Seleccionar un color del cable y soldarlo al pin 1 y el 6 del conector DB-9 (del lado del conector, se deben puentear estos pines con un pequeño trozo de cable).
B. Soldar otro cable al pin 2, otro al 3 y así sucesivamente hasta el 9.
C. El pin 9 debe dejarse vacío.
D. Soldar los cables sobrantes en cualquier lugar de la parte metálica, para evitar que las señales electromagnéticas interfieran en la señal que fluye por la línea.
E. Anotar en un borrador el color de cada cable y a qué pin fue soldado.

5) En el otro extremo del cable serial (la otra ficha DB-9) soldaremos los pares trenzados de la siguiente forma:
   A. El cable que fue soldado al pin 1 y 6, lo soldamos al pin 4
   B. El que fue soldado al pin 2, va soldado al pin 3
   C. El cable soldado al pin 3, lo soldamos al pin 2
   D. El que fue al pin 4, lo soldamos al 1 y el 6, armando nuevamente un puente para este extremo.
   E. El que fue al pin 5, en este extremo lo conectamos nuevamente al pin 5.
   F. El que fue al pin 7, lo soldamos al pin 8
   G. El que fue al pin 8, lo soldamos en el pin 7.

H. Nuevamente nos queda el pin 9 vacío, y el sobrante lo conectamos en cualquier sitio de la parte metálica.

El estándar general para este extremo del cable DB-9 debería ser de la siguiente forma:




*(Imagen obtenida del blog La Web Inteligente)*

6) Antes de armar cada extremo del conector DB-9 dentro de su caja, es conveniente que coloquemos silicona en cada uno de los pines soldados, para protegerlos.
7) También es recomendado medir con un tester cada cable, para asegurarse de que esté bien soldado y que no esté haciendo puente con otro cable.
8) Por último, únicamente queda armar cada extremo del cable dentro de su caja, teniendo cuidado de que cada cable pelado quede dentro de su caja.

## Conectando equipos a través de módem nulo

Una vez conectadas las 2 computadoras con el cable módem nulo nuevo que tenemos armado, podemos ya conectar cada PC a un extremo del cable y probar la conexión. Para esta etapa, además de realizar la conexión por Hardware necesitaremos realizar conexión a través de Software. Como la comunicación se realizará por puertos seriales, si bien Windows ya incluye el controlador para que los equipos se reconozcan, es necesario utilizar una terminal como Telix, Interlink o Hiperterminal.

Debemos crear en el Software elegido una nueva conexión que se realizará al puerto de comunicaciones que corresponda (generalmente será COM 1) y procedemos a configurar ambas computadoras con las mismas características para la transferencia de datos:

- 9600 bits por segundo
- 8 bits de datos

- Paridad nula
- 1 bit de parada
- Control de flujo, nulo.
- La configuración de la terminal deberá en ambos equipos, estar marcada con emulación de tipo ANSI.
- En la configuración de los caracteres ASCII debemos activar el modo eco de los caracteres escritos localmente, con el fin de poder ver lo que estamos escribiendo.
- Enviar un mensaje desde la terminal y observar si se recibe desde el otro equipo.

## Velocidad de transmisión de datos a través del módem nulo:

Entre sus limitaciones, cabe destacar que el módem nulo tiene una limitación de velocidad de transferencia de datos que proviene del estándar del protocolo RS-232 que es la interfaz a la cual nos estamos conectando.

El protocolo RS-232 establece que la transmisión usa entre 5 y 8 bits de datos, con una velocidad de transmisión de entre 100 y 900 kbaudios. Al configurar las terminales en Windows, uno de los parámetros a seleccionar es la velocidad de transferencia de datos. Si seleccionamos 9600 bps la velocidad será de 9600 bits por segundo, o lo que es lo mismo 1200 Bytes por segundo. Esta tasa es bastante baja, podríamos decir que extremadamente baja teniendo en cuenta las velocidades que manejan las redes en la actualidad.

Sin embargo, podemos realizar algunas pruebas y análisis y ver qué ocurre al transmitir mensajes desde la terminal, por ejemplo:

- Colocar una velocidad diferente en cada equipo.
- Probar conectar un equipo con una velocidad de 9600 bps mientras que el otro colocarle una cifra mucho mayor, por ejemplo 32000 bps, y observar lo que sucede (deberíamos experimentar errores en la recepción de los mensajes).

*Información, imágenes y más análisis y pruebas con Hyperterminal en: Tuelectrónica*

# Sumergiéndonos en las redes de computadoras: Conmutación y ruteo

En este apartado vamos a trabajar aspectos relacionados a las redes que conocemos en la actualidad, y su funcionamiento básico en relación con otras redes. Cabe aclarar que es posible realizar conexiones entre diferentes redes, incluso en redes de diferentes tipos o dimensiones, construyendo lo que conocemos como **interred.** Internet es el mayor ejemplo de ello.

## Conmutación

Para el abordaje de los contenidos que siguen utilizaremos mucho este concepto, diremos que conmutación es la acción de establecer una vía, o un camino entre dos puntos concretos, uno de ellos es un emisor -que llamaremos T(x) – y un receptor –al que llamaremos R(x)- a través de determinados nodos o puntos concretos intermedios. La conmutación permite la entrega de señales desde el emisor al receptor, pasando por todos esos nodos intermedios.

## Conmutación, numeración y ruteo en redes telefónicas:

Para el enrutamiento de redes se utilizan de forma inevitable protocolos de comunicación, en el caso de redes telefónicas, los más comunes son por ejemplo RIP, OSPF y BGP, veremos a continuación cómo funciona cada uno básicamente.

Antes de ello, debemos entender el concepto de **backbone** (columna vertebral en Inglés), el cual puede interpretarse como las principales conexiones troncales de Internet. Están compuestas de un gran número de  interconectados comerciales, gubernamentales, universitarios y otros de gran capacidad que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.

<u>*RIP (Routing information protocolo, protocolo de información de encaminamiento)*</u>

*RIP es un protocolo de encaminamiento interno, es decir para la parte interna de la red, la que no está conectada al backbone de Internet. Es muy usado en sistemas de conexión a internet como lo son las ISP, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.*

*Cuando un usuarios se conecta el servidor de terminales (equipo en el que finaliza la llamada) avisa con un mensaje RIP al router más cercano advirtiendo de la dirección IP que ahora le pertenece.*

*Así podemos ver que RIP es un protocolo usado por distintos routers para intercambiar información y así conocer por donde deberían enrutar un paquete para hacer que éste llegue a su destino.*

<u>*OSPF (Open shortest path first, El camino más corto primero)*</u>

*OSPF se usa, como RIP, en la parte interna de las redes, su forma de funcionar es bastante sencilla. Cada router conoce los routers cercanos y las direcciones que posee cada router de los cercanos. Además de esto cada router sabe a que distancia (medida en routers) está cada router. Así cuando tiene que enviar un paquete lo envía por la ruta por la que tenga que dar menos saltos.*

*Así por ejemplo un router que tenga tres conexiones a red, una a una red local en la que hay puesto de trabajo, otra (A) una red rápida frame relay de 48Mbps y una línea (B) RDSI de 64Kbps. Desde la red local va un paquete a W que está por A a tres saltos y por B a dos saltos. El paquete iría por B sin tener en cuenta la saturación de la línea o el ancho de banda de la linea.*

*La O de OSPF viene de "Open" abierto, en este caso significa que los algoritmos que usa son de disposición pública.*

*BGP (Border gateway protocol, protocolo de la pasarela externa)*

*BGP es un protocolo muy complejo que se usa en la interconexión*

*de redes conectadas por un backbone de internet. Este protocolo usa parámetros como ancho de banda, precio de la conexión, saturación de la red, denegación de paso de paquetes, etc. para enviar un paquete por una ruta o por otra. Un router BGP da a conocer sus direcciones IP a los routers BGP y esta información se difunde por los routers BGP cercanos y no tan cercanos. BGP tiene su propios mensajes entre routers, no utiliza RIP.*

*BGP es usado por grandes proveedores de conectividad a internet.*

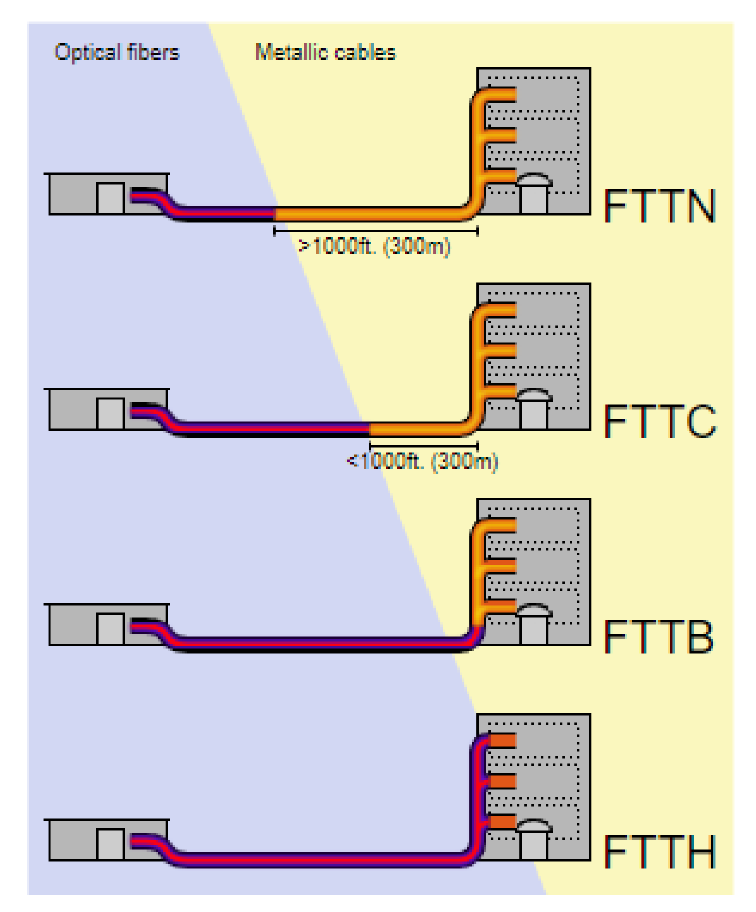
(Artículo de la Universidad de Málaga)

## Redes FTTH

Con la aparición de la fibra óptica, la velocidad de las redes sufrió un cambio drástico que se ha venido incrementando a ritmo vertiginoso y los que habitamos en Latinoamérica lo hemos experimentado a partir de la década del 2010. FTTH significa *"Fiber to the Home"*, lo que en Inglés significa "Fibra hasta la casa" y se encuentra enmarcada dentro de las tecnologías de redes de fibra óptica FTTx. se basa en utilizar cables de  y sistemas de distribución ópticos adaptados a esta tecnología para distribuir servicios avanzados, como el paquete de televisión por cable, telefonía e Internet, a los hogares y negocios de los abonados.

La implantación de esta tecnología ha estado tomando fuerza en los últimos años, especialmente en países como Chile, España, Estados Unidos, Colombia, Uruguay, Japón y países de Europa. Muchos operadores reducen la promoción de servicios  en beneficio de la fibra óptica con el objetivo de proponer servicios muy atractivos de banda ancha para el usuario (música, vídeos, fotos, etc.).

Las tecnologías FTTx suelen utilizar cables de fibra óptica desde el router del proveedor hasta los hogares, pero en las instalaciones finales (las terminaciones a las PC) se utiliza el tradicional cable par trenzado de cobre. En la siguiente imagen podemos ver cómo lo implementa cada tecnología:




*(Imagen obtenida de Wikipedia).*

## Modulación AM, FM y QM

Anteriormente ya hablamos del concepto de modulación, ahora que estamos profundizando en redes de computadoras, cabe detallar un poco sobre cómo es el proceso de modulación en diferentes tipos de ondas portadoras.

Debemos recordar el concepto de **onda portadora**, las cuales recordemos, son ondas de radio, por lo general de tipo sinusoide que han sido modificadas para enviar información. Los conocidos métodos como modulación de amplitud (AM) y de frecuencia (FM) son ejemplos de esto, y procederemos a desarrollarlos a continuación.

### ***Modulación de Amplitud (AM)***

*Modulación de amplitud (AM es el proceso de cambiar la amplitud de una portadora de frecuencia relativamente alta de acuerdo con la amplitud de la señal modulante (información). Las frecuencias que son lo suficientemente altas para radiarse de manera eficiente por una antena y propagase por el espacio libre se llaman comúnmente*

*radiofrecuencias o simplemente RF. Con la modulación de amplitud, la información se imprime sobre la portadora en la forma de cambios de amplitud.*

*La modulación de amplitud es una forma de modulación relativamente barata y de baja calidad de modulación que se utiliza en la radiodifusión de señales de audio y vídeo. La banda de radiodifusión comercial AM abarca desde 535 a 1605 kHz. La radiodifusión comercial de tv se divide en tres bandas (dos de VHF y una de UHF).*

*Los canales de la banda 1 entre 2 y 6 (54 a 88 MHz), los canales de banda alta de VHF son entre 7 MHz) y los canales de UHF son entre 14 a 83 (470 a 890 MHZ). La modulación de amplitud también se usa para las comunicaciones de radio móvil de dos sentidos tal como una radio de banda civil (CB) (26.965 a 27.405 MHz).*

*Un modulador AM es un aparato no lineal con dos señales de entrada de información: una señal portadora de amplitud constante y de frecuencia sencilla, y la señal de información. La información actúa sobre o modula la portadora y puede ser una forma de onda de frecuencia simple o compleja compuesta de muchas frecuencias que fueron originadas de una o más fuentes. Debido a que la información actúa sobre la portadora, se le llama señal modulante. La resultante se llama onda modulada o señal modulada.*

***Desventajas***

*Como un medio para transmitir información, la modulación de amplitud tiene muchas ventajas; sin embargo, también presenta algunas desventajas que, en ciertas condiciones, limitan su utilidad y obligan a buscar otras formas de modulación. La desventaja principal de la modulación de amplitud estriba en que la afectan fácilmente diversos fenómenos atmosféricos (estática), señales electrónicas con frecuencias parecidas y las interferencias ocasionadas por los aparatos eléctricos tales como motores y generadores.*

*Todos estos ruidos tienden a modular en amplitud la portadora, del mismo modo que lo hace su propia señal moduladora. Por lo tanto se convierten en parte de la señal modulada y subsisten en ella durante todo el proceso de demodulación. Después de la demodulación se manifiestan como ruido o distorsión, que si es bastante fuerte, puede sobreponerse a toda la información y hacer completamente inaprovechable la señal demodulada. Aun si aquellos no son tan acentuados como para tapar parte de la información, sí pueden ser extremadamente molestos.*

(Electronicafacil)

***Frecuencia Modulada (FM)***

*Consiste en variar la frecuencia de la onda portadora de acuerdo con la intensidad de la onda de información. La amplitud de la onda modulada es constante e igual que la de la onda portadora. Datos digitales pueden ser enviados por el desplazamiento de la onda de*

*frecuencia entre un conjunto de valores discretos, una modulación conocida como modulación por desplazamiento de frecuencia.*

***Utilidad***

- *Se utiliza en frecuencias intermedias de la mayoría de los sistemas de vídeo analógico, incluyendo VHS, para registrar la luminancia (blanco y negro) de la señal de video.*
- *Para la grabación de video y para recuperar de la cinta magnética sin la distorsión extrema, como las señales de vídeo con una gran variedad de componentes de frecuencia - de unos pocos hercios a varios megahercios.*
- *Mantiene la cinta en el nivel de saturación, y, por tanto, actúa como una forma de reducción de ruido del audio, y un simple corrector puede enmascarar variaciones en la salida de la reproducción, y que la captura del efecto de FM elimina a través de impresión y pre-eco.*
- *En las comunicaciones, la mejora de un sistema de transmisión y recepción en características como la relación señal – ruido, sin duda es uno de los más importantes, pues permite una mayor seguridad en las mismas.*
- *En las frecuencias de audio para sintetizar sonido. Está técnica, conocida como síntesis FM, fue popularizada a principios de los sintetizadores digitales y se convirtió en una característica estándar para varias generaciones de tarjetas de sonido de computadoras personales.*

(EcuRed)

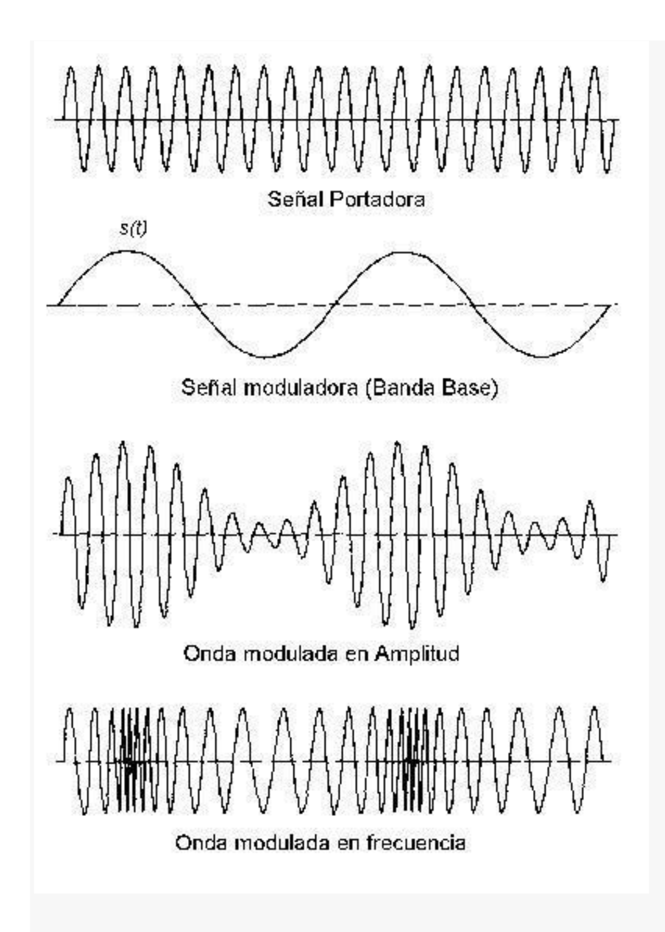



*Imagen extraída de [Erikrz]*

*Modulación de Amplitud en Cuadratura (QAM):*

*La modulación de amplitud en cuadratura o QAM (acrónimo de Quadrature Amplitude Modulation, por sus siglas en inglés) es una técnica que transporta dos señales independientes, mediante la  de una señal portadora, tanto en amplitud como en fase. Esto se consigue modulando una misma portadora, desfasada en 90. La señal modulada en QAM está compuesta por la suma lineal de dos señales previamente moduladas en doble banda lateral con portadora suprimida .*

*Se asocian a esta tecnología aplicaciones tales como:*

- *Modems telefónicos para velocidades superiores a los 2400 bps.*
- *Transmisión de señales de televisión, microondas, satélite (datos a alta velocidad por canales con ancho de banda restringido).*
- *Modulación con codificación reticulada, que consigue velocidades de transmisión muy elevadas combinando la modulación con la codificación de canal.*
- *Módems ADSL que trabajan a frecuencias comprendidas entre 24 KHz y 1104 KHz, alcanzándose velocidades de datos de hasta 9 MB/s.*

(Wikipedia)

# Algunos cálculos: Ancho de banda y logaritmos

Para el abordaje de este tema va a ser necesario emplear técnicas de una disciplina abstracta y formal que ha permitido el desarrollo de casi todas las demás disciplinas: La matemática, en particular, el análisis matemático. Con el fin de facilitar el trabajo, se ha intentado para este documento buscar la manera más sencilla de su abordaje, pero para comprender aspectos relacionados al ancho de banda de cualquier canal de comunicación, es necesario dedicarle un espacio, en particular al estudio de los logaritmos.

Para estudiar señales analógicas, es imprescindible comprender lo que es el ancho de banda que las mismas puedan tomar, y para ello existen varias técnicas; algunas de ellas, incluyen fundamentos matemáticos de considerable complejidad, que incluyen, por ejemplo, integración. Siendo que este documento está orientado al apoyo en el estudio de cualquier persona que se encuentre incursionando en redes y telecomunicaciones, pero en particular para estudiantes cuyo nivel es de Segundo Año de Bachillerato, se ha optado por desarrollar aquellas técnicas que no requieran integración y cálculos de nivel universitario, pero sí se trabajarán otras operaciones, como el caso de los mencionados logaritmos. Explicaremos algunos conceptos brevemente y a continuación ya nos aproximaremos a trabajar con estos puntos.

## Decibelio

Al trabajar con los temas que se desarrollaran a continuación, tendremos que manejarnos con una unidad de la que seguramente todos hayamos escuchado en algún momento, pero cabe detallar de qué se trata, y es el Decibel o Decibelio (dB). Se utiliza en magnitudes acústicas y electrónicas, pero no se trata de una unidad de medida propiamente dicha, sino de una unidad que muestra una relación entre dos potencias. La unidad original es el Bel (B) pero debido a la gran amplitud de los campos que se miden en la práctica, se utiliza un múltiplo de esta unidad, que es precisamente el dB.

La relación es la siguiente:

1B = 10 dB y representa un aumento de potencia de 10 veces sobre la magnitud de referencia. 0B es la magnitud de referencia que tomemos, entonces encontramos por ejemplo que:

- 2 B = 100 veces el valor de la magnitud de potencia
- 3 B = 1000 veces el valor de la magnitud de potencia
- Y así sucesivamente… Por ello se utiliza el dB, que permite incrementar estas relaciones con una razón de incremento 10 veces menor, que igualmente no deja de ser alta. Por ejemplo, un artefacto que trabaje emitiendo un sonido de 40 dB, no es “un poco” más ruidoso que uno que emita 30dB, es 10 veces más “ruidoso”. Y no emite el doble de sonido de uno que emite 20 dB, sino que es 100 veces más ruidoso.

- Cabe resaltar, que el dB (o el B) no representan una cantidad en sí, sino una **relación entre cantidades**, la cual va a depender de la cantidad original que se tome como referencia.

Más adelante volveremos a abordar este tema y veremos que en realidad, es una unidad logarítmica y escalar.

## Ancho de Banda

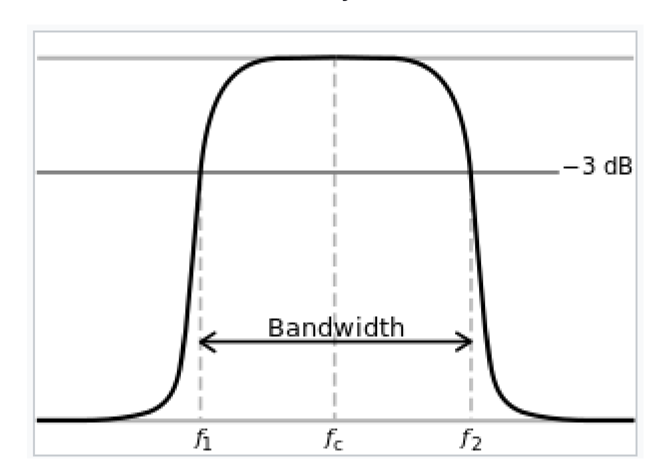
En computación y en particular en las redes, suele llamarse comúnmente **ancho de banda** al ancho de banda digital, es decir, la medida de datos y recursos de comunicación disponible o consumida. Básicamente se expresa en bits por segundo (bps) o en sus múltiplos Kbit/s, Mbit/s, etc.

Esta definición no está mal, pero la dejaremos de lado por un tiempo ya que es de uso coloquial, y si estamos hablando de **señales** y frecuencias, no nos sirve y nos puede llevar a confusiones.

Si estamos hablando de señales analógicas, el **ancho de banda** es la extensión, medida en Hz de las frecuencias en las que se concentra la mayor potencia de la señal. Las frecuencias que se encuentran dentro de este límite son las que conocemos como **frecuencias efectivas.**

Una señal periódica de una sola frecuencia tiene un ancho de banda mínimo. En general, si la señal periódica tiene componentes en varias frecuencias, su ancho de banda es mayor, y su variación temporal depende de sus componentes frecuenciales.

En la siguiente imagen (extraída de Wikipedia) podemos tener una básica representación del ancho de banda que se encuentra determinado por las frecuencias comprendidas entre las frecuencias f1 y f2:




## Logaritmos

En primer lugar es preciso aclarar por qué se utiliza logaritmos para representar medidas frecuenciales, en particular en relación con el ancho de banda, existen al menos dos razones fundamentales para que así sea, una de carácter histórico y una de carácter práctico:

- Desde el comienzo de la telefonía, se descubrió que la respuesta del oído humano a la intensidad sonora es de tipo logarítmico.

- En electrónica y en particular en telecomunicaciones, se manejan magnitudes de voltaje, corriente y potencia en rangos muy altos, tanto que sería complicado trabajar con unidades de medida tradicionales. La curva de incremento de la función logaritmo, resulta excelente para su representación.

Sin más, pasamos a aclarar lo que es un logaritmo y luego trabajaremos algunas identidades logarítmicas, que nos servirán para cálculos a futuro.

Definición:

*Dado un número real (argumento x), la función logaritmo le asigna el exponente n (o potencia) a la que un número fijo b (base) se ha de elevar para obtener dicho argumento. Es la función inversa de b a la potencia n. Esta función se escribe como: n = log*$_b$ *x, lo que permite obtener n.*

$$\log_b x = n \quad \Leftrightarrow \quad x = b^n$$

(Esto se lee como: logaritmo en base *b* de *x* es igual a *n*; si y sólo si *b* elevado a la *n* da por resultado a *x*.)

(Wikipedia)

No entraremos en detalle de las propiedades logarítmicas porque la intención del trabajo es resumir los contenidos a modo de entender los temas relacionados más estrechamente con redes y telecomunicaciones, sin profundizar en el campo de las matemáticas, pero es recomendado para el lector profundizar en las propiedades logarítmicas y practicarlas si no las ha estudiado anteriormente.

## Identidades logarítmicas

Las identidades que se detallarán a continuación son igualdades que se podrán aplicar para simplificar algunos cálculos:

$$\log_b(xy) = \log_b(x) + \log_b(y) \quad \text{porque} \quad b^x \cdot b^y = b^{y+x}$$

$$\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y) \quad \text{porque} \quad \frac{b^x}{b^y} = b^{x-y}$$

$$\log_b(x^y) = y \log_b(x) \quad \text{porque} \quad (b^x)^y = b^{xy}$$

$$\log_b(\sqrt[y]{x}) = \frac{\log_b(x)}{y} \quad \text{porque} \quad \sqrt[y]{b^x} = b^{x/y}$$

Cancelación de exponentes

Por deducción, sabemos que los exponenciales son la operación inversa al logaritmo, es lo que llamamos un antilogaritmo.

$$b^{\log_b(x)} = x \quad \text{porque} \quad \text{antilog}_b(\log_b(x)) = x$$

$$\log_b(b^x) = x \quad \text{porque} \quad \log_b(\text{antilog}_b(x)) = x$$

Cambio de base

$$\log_a b = \frac{\log_c b}{\log_c a}$$

Donde *c* es una constante cualquiera, es decir, cualquier base válida (de hecho la base por defecto que tiene la función logaritmo de nuestra calculadora es 10).

## Relaciones logarítmicas de potencia:

Para establecer las relaciones logarítmicas de potencia medidas en Bels (B), se ha tomado como referencia un artículo de la Universidad de Cantabria, el cual se copia y referencia debajo:

$$P_{LOG} = \log_{10}\left(\frac{W}{W_{ref}}\right) \; bels \qquad (2.1)$$

Donde $W$ es la potencia en watts, miliwatts, etc. y $W_{ref}$ es el valor de potencia usada como referencia. La expresión anterior no se utiliza y, en su lugar es más común la expresión de *decibeles*:

$$P_{dB} = 10\log_{10}\left(\frac{W}{W_{ref}}\right) \quad \text{decibeles (dB)} \qquad (2.2)$$

En lo sucesivo, omitiremos la designación $log_{10}$ y usaremos simplemente *log*, ya que en todos los casos se trata de logaritmos base 10. Cuando se trate de logaritmos naturales se usará la designación *ln*. Aunque la potencia de referencia puede ser cualquiera, lo común es utilizar como tal 1 w, 1 mw ($10^{-3}$ w), 1 pw ($10^{-9}$ w) y 1 Kw ($10^{3}$ w), lo que da lugar a las siguientes designaciones:

*dBw* $\rightarrow$ Nivel de potencia en dB, referido a 1 w.

*dBm* $\rightarrow$ Nivel de potencia referido a 1 mw.

*dBpw* $\rightarrow$ Nivel de potencia referido a 1 pw.

*dBKw* $\rightarrow$ Nivel de potencia referido a 1 Kw

(Unican)

## Ganancia

Cuando trabajamos con señales eléctricas, la ganancia establece la relación entre dos niveles de voltaje, potencia o corriente de entrada y salida en un circuito o sistema cualquiera. Podemos por ejemplo, hablar de la ganancia en W que ofrece un amplificador de sonido entre la potencia que recibe y la que emite, en breves líneas abordaremos este ejemplo.

Si bien el concepto de ganancia es adimensional, es decir, se aplica a varios campos, se refiere a determinada magnitud, vemos a continuación cómo se calcula la ganancia de potencia, voltaje (tensión) y corriente (intensidad).

- **Ganancia de potencia**, definida como $G_P = \frac{P_{\text{salida}}}{P_{\text{entrada}}}$ y expresada en decibeles es $G_P(\text{dB}) = 10 \cdot \log \frac{P_{\text{salida}}}{P_{\text{entrada}}}$
- **Ganancia en tensión**, de forma similar a la anterior: $G_V = \frac{V_{\text{salida}}}{V_{\text{entrada}}}$ y expresada en decibeles es $G_V(\text{dB}) = 20 \cdot \log \frac{V_{\text{salida}}}{V_{\text{entrada}}}$
- **Ganancia en corriente**, de forma similar a la anterior: $G_I = \frac{I_{\text{salida}}}{I_{\text{entrada}}}$ y expresada en decibeles es $G_I(\text{dB}) = 20 \cdot \log \frac{I_{\text{salida}}}{I_{\text{entrada}}}$

Es importante aclarar que, si el resultado de la ganancia es **negativo**, se le denomina **atenuación.**

### Ganancia utilizando valores de potencia:

Veremos un ejemplo concreto, el que se mencionaba antes, del amplificador:

- Supongamos que un amplificador ofrece una salida de 50W, con una entrada de 20W, la ganancia en dB será de 10 * Log(50/20) = 3,9794 dB
- En el ejemplo anterior, si la potencia de entrada fuera de 50W y la de salida de 20W, la ganancia en dB sería de 10* Log(20/50) = -3,9794 dB, por lo cual no podríamos hablar de una ganancia con ese resultado, sino de una **atenuación** de 3,9794 dB

### Ganancia utilizando valores de voltaje:

Ahora veremos otra aplicación de la ganancia, como antes se detalló, también es posible encontrar la ganancia en valores de tensión, y también se expresa en decibeles. Repasando, $G_V$ = V (Salida) / V (entrada).

**Importante:** Cuando se trabaja con tensión, sabemos que el voltaje puede sufrir sensibles variaciones, y cuando trabajamos con corriente alterna, estas variaciones incluso significan cambio de polo, por lo cual introduciremos un par de conceptos:

- Valor de pico (Vp) que refiere al valor máximo de tensión que podemos esperar.
- Valor de pico – pico (Vpp) que refiere a la diferencia entre el pico máximo positivo y el máximo negativo que podemos encontrar en nuestro sistema.

Sin más, desarrollaremos nuestro ejemplo:

- Si un amplificador tiene una entrada de 0.2 Vpp (voltios pico – pico) y una salida de 10 Vpp, la ganancia de tensión será de: 20 * Log(20/0.2) = 33,9794 dB.

## Ejercicios

- Determinar la ganancia o atenuación correspondiente a un amplificador de sonido que recibe una entrada de 5W de potencia y una salida de 20W.
- Determinar la ganancia o atenuación correspondiente a un amplificador de sonido que recibe una entrada de 20W y una salida de 40W.
- Determinar la ganancia o atenuador de un atenuador que recibe 220 Vpp y la salida es de 12 Vpp.

## Capacidad del Canal:

En Electrónica se le llama capacidad del canal a la cantidad de información que puede ser transmitida sobre un canal de comunicación (Recordemos que, el canal de comunicación es el medio por el cual viajan las señales portadoras de información entre un emisor y un receptor).

La capacidad del canal se mide en bps (bits por segundo) y depende del **ancho de banda** y de la **relación señal / ruido.** Este resultado limita la cantidad de información que puede transmitir una señal que se envía a través de dicho canal.

- Lógicamente, lo deseable es tener mayor capacidad de canal para poder tener mayor velocidad de transmisión de datos, el enemigo fundamental para lograrlo es el ruido, que se entiende por interferencias al canal que distorsionan la señal. A menor ruido y mayor ancho de banda, el canal tendrá mayor capacidad, pero también será lógicamente más costoso.

<u>Fórmula para calcular la capacidad del canal</u>

**Importante: Para las fórmulas que se presentarán en este tema se ha optado por utilizar el símbolo asterisco (*) para representar la multiplicación. Esto se debe a que en el lenguaje informático se suele utilizar para multiplicar y se asume que separarlo de éste modo ofrecerá una mayor comprensión al lector que se encuentra familiarizado con esta simbología.**

- Teniendo en cuenta que C es la capacidad máxima del canal que queremos calcular, y que B es el ancho de banda (medido en Hz), C se calcula siguiendo la siguiente fórmula:

$$C \text{ (bps)} = B * \text{Log}_2 (1 + S/R)$$

<u>Régimen Binario de una Señal:</u>

El régimen binario de una señal no puede ser mayor que la capacidad de ese canal y depende del número de niveles o estados que se utilizan para codificar la información, su fórmula consta de los siguientes elementos:

- Llamaremos n al número de bits por cada elemento de la señal.

- Llamaremos M al conjunto de elementos diferentes que puede adoptar una señal (se entiende también como los niveles de una señal)
- C es la capacidad del canal resultante.

El régimen binario de una señal (nVt) se mide en baudios, y puede calcularse del siguiente modo:

$$nVt = 2 * B * n = 2 * B * \log_2 M = C \text{ (bps)}$$

La propuesta anterior parte de lo que se conoce como Teorema de Nyquist, y supone un canal sin ruido, es decir, un canal ideal. Veamos algunos ejemplos prácticos:

- Si suponemos que un canal de voz con un ancho de banda de 3100 Hz se utiliza con un módem para transmitir datos digitales ( 2 niveles). la capacidad C del canal es 2 * B (3100 Hz) * ($\log_2$ 2) = 6200 bps.

**Ejercicios**

- Calcule la capacidad de un canal de un modem de 12400 Hz, para transmitir datos digitales (2 niveles) a través de un canal ideal (donde la relación S/R es de 1, es decir, sin ruido).
- Calcule la capacidad de un canal con un ancho de banda de 6200 Hz que se usa para transmitir datos en 4 niveles, y con una relación S/R de 0,8 dB.

## Ejercicios para evaluar una primera introducción a las Redes

Hasta el momento este documento se ha enfocado en una introducción con una importante cantidad de contenido teórico, acercándose sobre el final a ejercicios de carácter práctico que pueden realizarse sin necesidad de herramientas específicas (excepto si se lo desea, armar un cable serial para modem nulo). Para resumir aspectos importantes de esta etapa, cabe responderse las siguientes cuestiones:

1) ¿Qué es una señal? Explicar brevemente cómo se clasifican.
2) ¿Cuál es la función que cumple un módem en una red telefónica?
3) Explique la funcionalidad de los códigos para detección de errores en señales de comunicación, y el funcionamiento de alguno de los algoritmos existentes.
4) ¿Qué son las redes FTTH?
5) Calcule la ganancia que existe en tres amplificadores diferentes de audio, si los tres reciben una potencia de entrada de 15 W, pero la salida ofrecida para cada amplificador es:
   a. 50 W
   b. 70W
   c. 80W
6) En redes y telecomunicaciones, ¿A qué se le llama capacidad del canal? Calcule la capacidad de un canal ideal cuyo ancho de banda es de 9600 Hz con 2 niveles de señal.

## Entrando en la arquitectura de las redes

Cuando hablamos de arquitectura de redes, nos referimos a cómo éstas están diseñadas y cómo se relacionan sus diferentes componentes entre sí. Las redes de computadoras se han vuelto cada vez más extensas y su uso se ha extendido a tal punto que parece inimaginable que una empresa con diferentes sucursales pueda existir sin tener una red instalada para la comunicación entre sus funcionarios, lo mismo con un ente público o con un instituto de educación. Para cada caso, los usuarios tendrán comunicación entre sí a través de redes construidas bajo una arquitectura diferente.

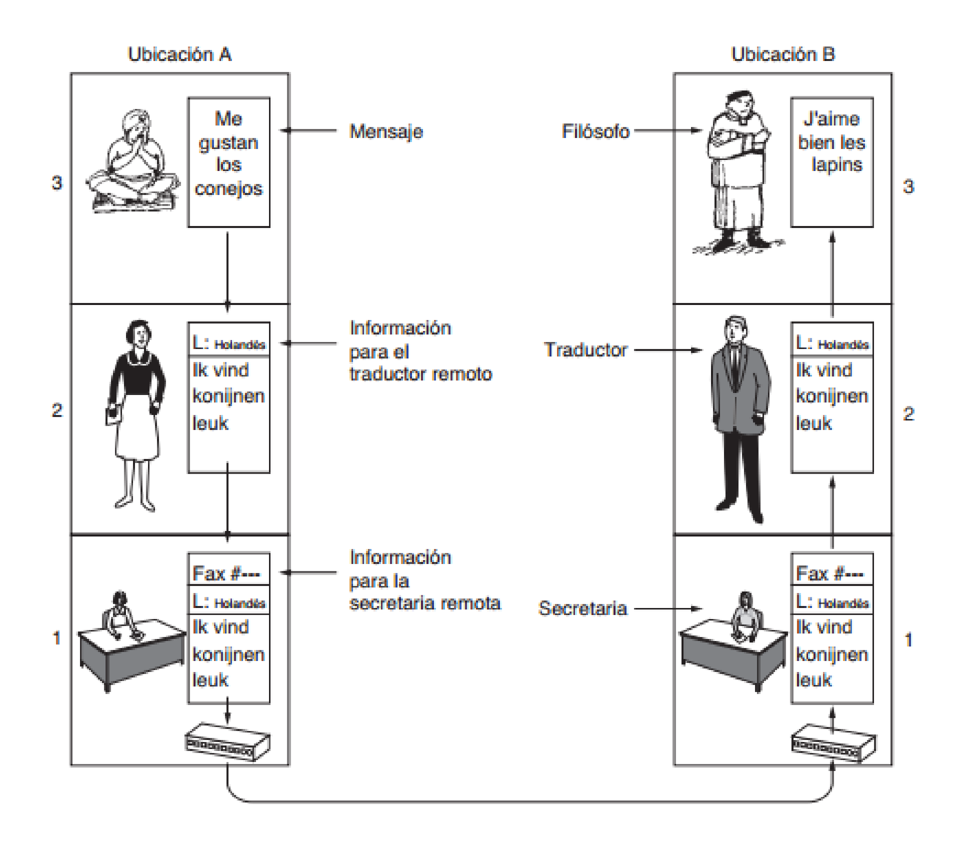
Antes de profundizar en el tema concreto, analicemos la siguiente analogía: ¿Cómo harían dos filósofos de diferentes culturas para interactuar entre sí, si se encuentran lejos y ninguno de los dos habla el idioma del otro? Supongamos que a su vez, cada filósofo tiene un traductor que habla su idioma pero además ambos traductores tienen una secretaria, con quien se pueden comunicar fluidamente y cada respectiva secretaria por su parte, hablan holandés y son las encargadas de realizar las llamadas telefónicas.

Uno de los filósofos (A) desea emitir un mensaje con una reflexión sobre la subjetividad de la ciencia, pero se encuentra en la India y únicamente habla el idioma hindi, entonces habla se lo transmite a su traductor, quien habla además holandés, y le avisa que ese mensaje va destinado a otro filósofo (B) que se encuentra en Francia y únicamente habla francés. Su traductor, traduce el mensaje del hindi al holandés, pero como no está encargado de hacer llamadas telefónicas se lo transmite a su secretaria, quien habla holandés y le indica para quién va destinado.

La secretaria realiza la llamada correspondiente a Francia y es atendida por la secretaria del filósofo B (que recordemos, habla francés) y comunicándose en holandés entre sí, le transmite el mensaje que va destinado para su filósofo.

La Secretaria del filósofo B, no habla su idioma, por lo que se lo dice a su traductor, quien finalmente toma el mensaje que originalmente A esbozó en hindi, y se lo transmite a su filósofo en francés, quien lo interpreta perfectamente sin hablar el idioma original.

La siguiente imagen ilustra el ejemplo anterior:




*(Imagen tomada de "Redes de Computadoras", Tanembaum 2014)*

En la siguiente analogía podemos observar que un mismo mensaje no se transmite entre ambos filósofos en un mismo idioma, ni tampoco se hace de forma directa, sino que pasa por intermediarios que transforman el mensaje según sea necesario para finalmente ser transmitido a un intermediario final, quien maneja el mismo idioma que su interlocutor del otro lado, donde se irá transformando el mensaje por cada intermediario en la escala superior hasta llegar al destinatario final.

## Protocolos, Capas y Servicios

En las redes de computadoras, las comunicaciones se dan en un esquema muy similar, existen **protocolos,** que como se mencionaba anteriormente, son acuerdos donde se establecen normas para establecer una comunicación entre interlocutores (en este ejemplo por ejemplo, el protocolo establecido entre las secretarias es hablar en holandés).

La comunicación a su vez, no se realiza en forma directa sino que se realiza a través de una escala de intermediarios, los que en términos de redes vamos a considerar como **capas**, las capas son los niveles jerárquicos entre los cuales se establece la comunicación. En el ejemplo cada capa tiene un intermediario que realiza su aporte al mensaje original, transformándolo o agregándole información de acuerdo a las necesidades para que sea interpretado del lado del interlocutor. Esa información a su vez, no es vista por miembros de capas superiores ya que no la necesita, el mensaje traducido de hecho sería incomprensible para ellos, por lo cual en cada nivel o capa de comunicación al mensaje original se le pueden agregar datos que son irrelevantes a otras capas, este concepto es el que se conoce como **encapsulamiento**, y es muy empleado en todas las ciencias computacionales, consta de prestar un servicio ocultando los detalles internos del mismo.

Los **servicios** son los métodos utilizados para que exista comunicación entre las diferentes capas, y la **arquitectura de red** en sí, será el conjunto de capas y servicios que conforman una red. Dicha arquitectura, es independiente de los detalles internos de cada computadora de la red, sus detalles de implementación son absolutamente transparentes a la implementación de hardware que se emplee en las máquinas, siempre y cuando las máquinas cuenten con la capacidad para comprender los protocolos instalados que se utilizarán en la comunicación.

Supongamos así, que podemos enviar mensajes a través de una red social desde una computadora, a un amigo que utiliza un teléfono móvil. Si bien las interfaces y características de ambos dispositivos son diferentes, el mensaje que enviamos pasa por todas las capas de comunicación correspondientes, es interceptada del otro lado y pasa por protocolos de comunicación con los que cuentan instalados ambos dispositivos.

En la actualidad, existen dos modelos de arquitecturas de redes, el modelo **OSI** (Open Systems Interconnection) diseñado por la Organización Internacional de Normas (ISO) que es ampliamente utilizado en la actualidad, pero cuyos protocolos se encuentran desactualizados, y el modelo **TCP/IP**, el cual por el contrario, se encuentra en desuso pero sus protocolos son ampliamente utilizados.

Para diseñar una arquitectura de red se debe tener en cuenta ambos modelos ya que, a nivel conceptual, la comprensión de lo que es una arquitectura de red es válida, y así se podrá también establecer comparaciones entre ambos modelos.

## El modelo OSI

Comprender la estructura de este modelo arquitectónico de red será lo que nos permitirá posteriormente entender la funcionalidad y la importancia de cada protocolo de red. Comprender los protocolos a su vez, resulta esencial, ya que en el lenguaje de las telecomunicaciones se mencionan de manera permanente, se utilizan para que efectivamente exista comunicación por lo que es nuestra tarea comprender bien cómo funciona esta estructura.

Veamos en principio un breve esquema del modelo OSI, con qué capas cuenta y posteriormente veremos cuáles son los protocolos que intervienen en cada capa, esto último lo detallaremos más adelante, pero primeramente debemos presentar cada capa y qué función cumple:

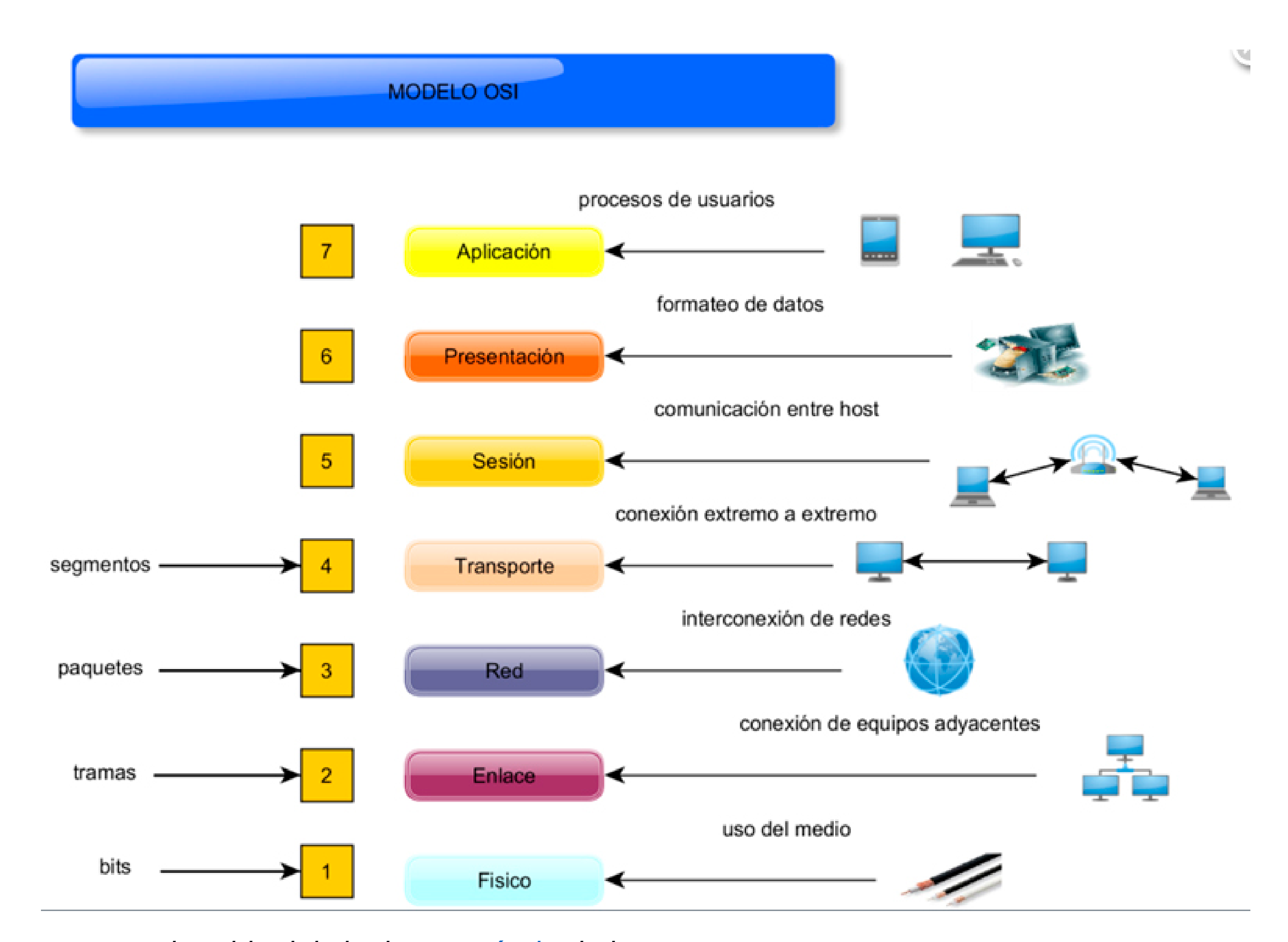



*Imagen obtenida del siguiente [artículo](#) de la UNAEH*

## Capas del modelo OSI

Para resumir y entender el funcionamiento de cada capa, vamos a presentarlas desde la más baja hasta la última. La capa más baja, en realidad no consiste en una capa del modelo OSI en sí misma, ya que el medio físico no depende del modelo sino del hardware que se esté utilizando. Los bits viajan a través del medio físico que puede ser cualquiera, incluso dentro de una misma red se pueden utilizar diferentes tecnologías dentro del medio físico (pueden haber en la red de una oficina, salas donde los equipos estén conectados por cable de fibra óptica, otros por cable par trenzado –UTP-, otra por WiFi, etc). Sin más, comenzaremos un pequeño análisis desde esta capa inferior del esquema, que para su estudio, puede trabajarse a la inversa, según las preferencias del lector.

### *Capa Física:*

Controla el acceso al medio, es decir, las señales por donde viajan los datos, que como ya se mencionó antes, depende de la tecnología que se esté utilizando. Esta capa sólo se encarga de transferencia de bits.

### *Capa de Enlace de Datos:*

Como el nombre nos lo indica, la capa de enlace se encarga de “enlazar” datos, es decir, direccionarlos, pero se ocupa de la dirección física de los datos dentro de la red independientemente de su topología, esta capa permite activar, mantener, deshabilitar la

conexión, como también notificar errores. El direccionamiento físico es quien emplea las direcciones de hardware (MAC) de los equipos.

*Capa de red:*

Se encarga de definir el camino que seguirán los datos desde el origen hasta su destino a través de una o más redes conectadas mediante dispositivos de enrutamiento (routers). A diferencia de la capa de enlace, la capa de red se encarga de realizar direccionamiento lógico, y es donde se toman en cuenta las direcciones IP de los equipos (IP es un protocolo de red ampliamente utilizado que detallaremos más adelante).

*Capa de transporte:*

Permite intercambiar datos entre sistemas finales, dividiendo el mensaje que proviene de las capas superiores en fragmentos, para luego enviarlo a la capa inferior (red) cuyo método puede variar. Existen servicios de la capa de transporte que son orientados a conexión y otros que no, es decir, algunos servicios se orientan en garantizar la seguridad e integridad de los datos, y otros se encargan de garantizar más velocidad de transferencia. El método a utilizar va a depender del fin para el cual se use y el protocolo, que se detallará más adelante.

*Capa de Sesión:*

Proporciona mecanismos para que exista comunicación entre las aplicaciones de las computadoras finales, encargándose de abrir, cerrar y mantener sesiones entre ambos sistemas.

*Capa de Presentación:*

Se encarga de definir el formato con el que se intercambian los datos entre aplicaciones, ofreciendo así un amplio conjunto de servicios para que los datos sean formateados y así comprendidos entre diferentes aplicaciones.

*Capa de Aplicación:*

Se encarga de proporcionar los servicios utilizados por las aplicaciones de los usuarios para que éstos se comuniquen entre sí a través de la red, es la capa de más alto nivel pues es la que interactúa con las aplicaciones de usuario, todas las capas inferiores a ella son transparentes a él.

Sólo a efectos de mencionar los protocolos de cada capa, se presenta la siguiente imagen, donde se los menciona según cada nivel del modelo OSI, su detalle será tarea para más adelante:

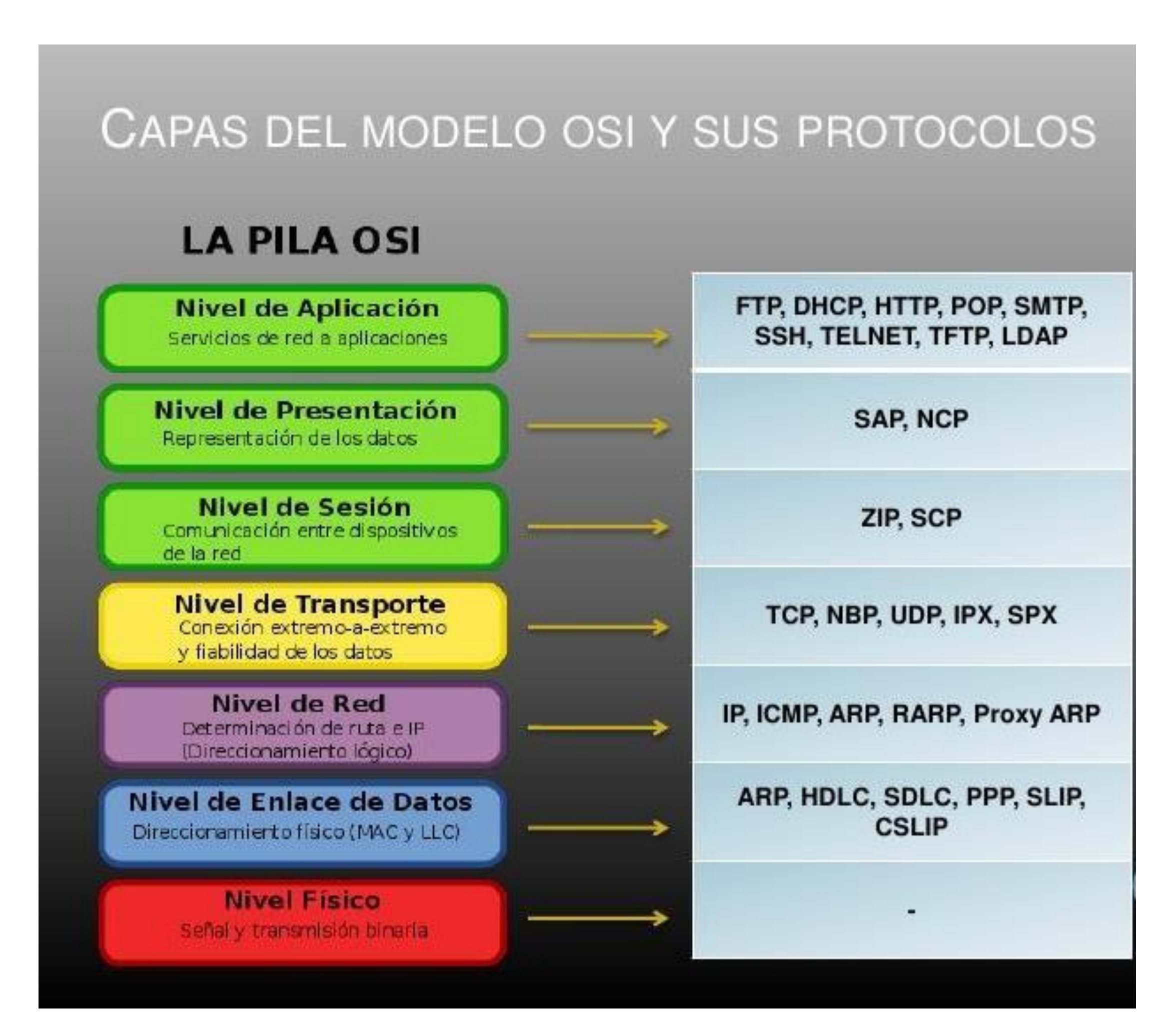



*Imagen obtenida del blog [Modeloosica]()*

## El modelo TCP/IP

Al igual que el modelo OSI, en cada capa del modelo TCP/IP se brindan servicios que ofrecen diferentes funcionalidades a sus capas superiores, pero, sin embargo, la arquitectura se encuentra dividida en cuatro capas y no en siete.

Para conceptualizarlo, podríamos decir en principio que el modelo TCP/IP resume algunas de las capas del modelo OSI, y elimina la capa física como tal, siendo que la diferencia entre capas es la que puede apreciarse en la imagen:

LA PILA OSI

Nivel de Aplicación
Servicios de red a aplicaciónes

Nivel de Presentación
Representación de los datos

Nivel de Sesión
Comunicación entre dispositivos de la red

Nivel de Trasporte
Conexión extremo-a-extremo y fiabilidad de los datos

Nivel de Red
Determinación de ruta e IP (Direccionamiento lógico)

Nivel de Enlace de Datos
Direccionamiento físico (MAC y LLC)

Nivel Físico
Señal y transmisión binaria

LA PILA TCP/IP

Nivel de Aplicación
HTTP, FTP, POP3, TELNET, SSH, ...

Nivel de Trasporte
Conexión extremo-a-extremo y fiabilidad de los datos
TCP, UDP

Nivel de Red
ICMP, IP, ARP, RARP, ...

Nivel de Enlace de Datos
Direccionamiento físico (MAC y LLC)

Nivel Físico
Señal y transmisión binaria

Al ver el esquema anterior, cualquier lector que no conozca demasiado pero reflexionando un poco sobre ambos esquemas, podría inferir lo siguiente: Si el modelo TCP/IP tiene menos capas pero es válido y fusiona capas del modelo OSI, ¿Por qué se los trata como modelos diferentes? ¿Por qué no hablamos siempre del modelo TCP/IP que parece más fácil?. Vamos a abordar la respuesta que diferencia bien estos modelos a continuación, así como el por qué del desuso de protocolos del modelo OSI, pero para empezar, debemos aclarar un principio fundamental en redes: **No es posible violar el modelo de capas, esto es, no puede haber comunicación entre protocolos de diferentes capas, sino que la información debe ser pasado entre capas a través de los servicios correspondientes.** Dicho esto, ocuparemos un espacio a diferenciar estos modelos y aclarar, por qué en la práctica, el modelo de referencia que se utiliza es OSI, sin embargo ya sus protocolos son obsoletos y se utilizan mayormente los protocolos del modelo TCP/IP.

- Implementar el modelo OSI sería muy complejo por su mala tecnología que lo hace incomprensible, *"junto con sus correspondientes definiciones y protocolos de servicios, es muy complejo. Si se apilan, los estándares impresos ocupan una fracción considerable de un metro de papel."* (Tanembaum, 2014). Se dice que el direccionamiento, el control de flujo y de errores en el modelo OSI aparecían en protocolos de varias capas diferentes
- El modelo OSI sufrió malas implementaciones, debido al problema tecnológico que ofrecía, aquellas que lo usaron consistieron en implementaciones pesadas y lentas, lo que hizo que las personas asociaran "OSI" con "mala calidad".
- El modelo TCP/IP era asociado con UNIX a comienzo de la década de los años 1980s, ya que UNIX hacía uso de este modelo para la manipulación de redes.

Dicho sistema operativo, fue considerado por esos años como el sistema de mejor funcionamiento y confiabilidad.

- El modelo TCP/IP tiene grandes debilidades de diseño, ya que la capa de transporte (donde combina transporte, sesión y presentación) no funciona como una capa sino como una interfaz entre las capas de red y la de aplicación.
- El modelo TCP/IP carece en realidad de una capa física, lo cual reduce el control sobre el acceso al medio.
- TCP/IP falla en aspectos de diseño como se decía anteriormente, y eso recae también en la generalidad, se hace imposible describir a través de este modelo cualquier pila de protocolos de cualquier sistema de redes. TCP/IP no es nada general en ese sentido, mientras que OSI sí lo es, no obstante, si observamos los protocolos listados en el esquema TCP/IP, veremos sin duda nombres que nos resultan familiares, son protocolos con buenas tecnologías que hoy día continúan utilizándose.

## Capas del modelo TCP/IP

Antes de profundizar demasiado en los protocolos y sus funcionalidades, vamos a hablar brevemente de las capas que conforman el modelo TCP/IP, así como se hizo anteriormente con el modelo OSI. En primer lugar, **aquí no tenemos una capa física,** obviamente existe señal y transmisión de datos binaria por medios físicos, pero hablaremos de **nivel físico** y no de una capa, por ello no se detallará a continuación.

### *Capa de Enlace o de Acceso a la Red:*

Para satisfacer las demandas de la capa superior, ésta, que es la de nivel más bajo de toda la pila TCP/IP, se encarga de efectuar un enlace físico entre los paquetes IP que provienen de la capa superior y los medios de red. En esta capa están incluidos los detalles de las tecnologías LAN y WAN (que abordaremos muy pronto), los de la capa física y de enlace de datos que se manejan en el modelo OSI.

En esta capa se definen los procedimientos para crear una interfaz entre un equipo terminal y el hardware de red.

### *Capa de Interred o Internet*

En el nivel donde en el modelo OSI ubicamos la capa de Red, en el caso de TCP/IP se establece la capa de Interred o simplemente llamada de "Internet". Ésta, es la capa más importante que mantiene unida toda la arquitectura de red, permite que desde todos los equipos hosts (clientes de la red) puedan inyectar paquetes de datos en cualquier red y viajen de manera independiente hasta su destino. Se encarga de interconectar redes incluso de diferentes dimensiones, de enrutar o encaminar los paquetes de datos dentro de dichas redes direccionándolos y empleando los protocolos necesarios para ese fin, entre ellos el más importante: El protocolo IP (Internet Protocol), el cual identifica a cada equipo dentro de una red. Este protocolo ha pasado por varias versiones, si bien el estándar es ipv4, la extensión de las redes ha generado problemas que se han subsanado en el paso de los años, pero no garantiza una IP para cada equipo como sí ocurre con ipv6 cuya implementación aún (2018) no se ha extendido realmente.

La analogía entre la capa de Interred con el mundo real es su comparación con un correo internacional convencional, donde un usuario puede dejar en una oficina de correos una lista de cartas para varias personas que se encuentran en diferentes países, cada carta viajará de manera independiente por diferentes agencias de correo intermedias, en países distintos, hasta llegar con un poco de suerte hasta su destino. Así los paquetes IP de un usuario pueden viajar por diferentes routers que los encaminarán hasta su destino final, el equipo hacia el cual van dirigidos.

Además de IP; la capa de interred define otro protocolo cuyo uso es ampliamente extendido que es ICMP (Protocolo de Control de Mensajes de Internet, del inglés "Internet Control Message Protocol") indispensable para el enrutamiento.

### *Capa de Transporte*

Esta capa funciona del mismo modo que la capa de Transporte en el modelo OSI, se encarga de establecer una comunicación entre equipos pares. Hace uso de dos protocolos fundamentales, TCP y UDP, pero antes de detallar sobre ellos, se hará una diferenciación entre servicios orientados a conexión y servicios sin conexión, para entenderlo del mejor modo.

#### Servicios orientados a Conexión

Son servicios donde se garantiza la integridad de los datos ya que los datos se transfieren a través de una conexión previamente establecida. El procedimiento es establecer la conexión, usarla todo el tiempo que sea necesario y luego cerrarla, pero el uso de la conexión y los recursos de red es exclusivo. Los servicios de red son reservados en ese momento para garantizar la calidad del servicio por el flujo constante de datos. La desventaja es que tanto la reservación del camino que cruzarán los datos como del ancho de banda se hacen de manera estática, manteniendo ocupada la vía de conexión y ralentizando la transferencia de datos.

#### Servicios sin conexión

Son aquellos donde el camino a seguir por los paquetes no se encuentra predeterminado y no se garantiza el secuenciamiento de paquetes, la tasa de transferencia de datos ni los recursos de la red. Cada paquete es transmitido independientemente por el sistema de origen y manejado independientemente por los dispositivos intermedios de la red. Las ventajas de este sistema es la selección dinámica del camino y la asignación dinámica de los recursos de red, teniendo como desventaja la fiabilidad de los datos que ofrecen los servicios con conexión.

Diferenciados ambos tipos de servicios, se entenderá mejor la diferencia entre los protocolos TCP y UDP.

- TCP (Transmission Control Protocol): Como su nombre lo indica, "Protocolo de Control de Transmisión", se encarga de asegurar y garantizar la transmisión de datos. Es un protocolo orientado a **conexión**, es decir, se encarga de garantizar la integridad de los datos que envía un emisor, asegurando que sea precisa con la información recibida por el receptor. Este protocolo segmenta el flujo de bytes entrante en mensajes discretos y los pasa cada uno a la capa de interred, en el

destino el receptor vuelve a ensamblar estos mensajes para formar el flujo de salida. TCP maneja también el control de flujo para evitar que un posible emisor rápido no inunde de mensajes a un receptor más lento, de modo tal que no los pudiese manejar.

- UDP (User Datagram Protocol): En español, su nombre significa "Protocolo de Datagramas de Usuario", es un protocolo **sin conexión,** donde no se establece control de flujo ni secuenciamiento de datos. Existen aplicaciones que utilizan este sistema por su rapidez, pero al no ser confiable deben manejar este tipo de servicios por su cuenta. Se utiliza en aplicaciones donde la entrega oportuna de mensajes es más eficiente que una entrega precisa, donde la velocidad es crucial, como en la transmisión directa de voz o video.

### *Capa de Aplicación*

El modelo TCP/IP carece de capas de sesión y presentación, las aplicaciones simplemente incluyen las funciones de sesión o presentación que requieran.

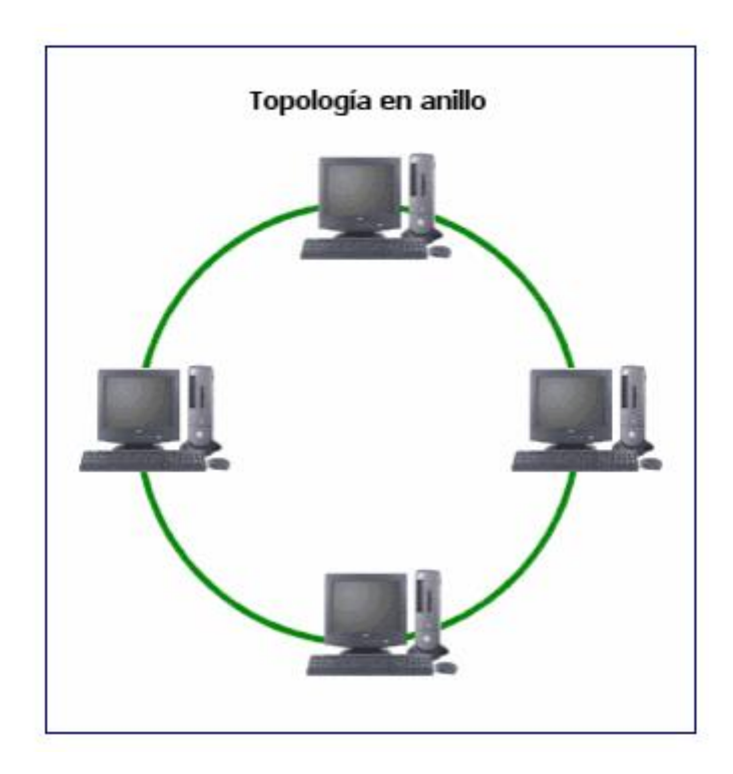
Esta capa es la de más alto nivel, por lo tanto, es quien tiene mayor interacción con el usuario, quien a su vez hace uso de las vistas de las aplicaciones para intercambiar información, la información pasa a su vez a la capa inferior para ser transferida, pero antes para por una serie de protocolos los que, dependiendo del caso, las aplicaciones seleccionan según su funcionalidad. Los protocolos de capa de aplicación incluyen los que permiten conectarse remotamente a un equipo (TELNET y SSH), transferencia de archivos (FTP), correo electrónico (POP3, SMTP, etc), sistema de nombres de dominio (DNS) para asociar nombres de hosts a direcciones de red y protocolos que proporcionen la recuperación de páginas de Internet (como HTTP y HTTPS).

## Clasificación de redes según su Topología

Se le llama **topología** de red a la forma de la distribución física que conforman las computadoras conectadas en una misma red. A continuación, pasaremos a clasificarlas.

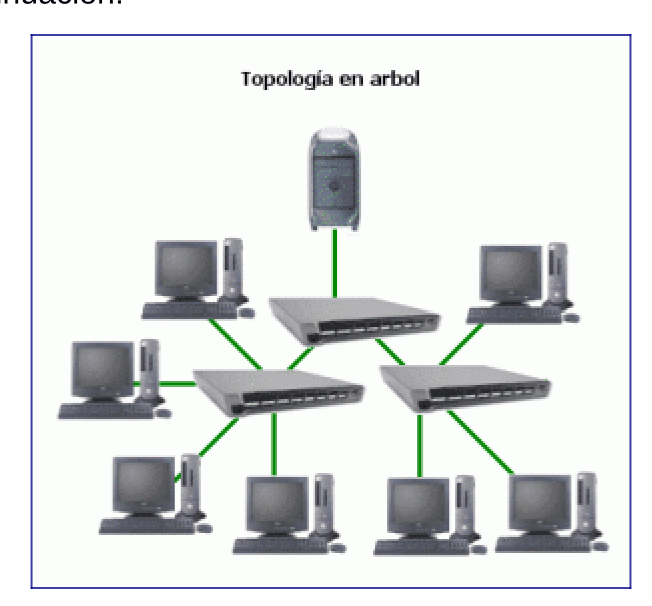
### Red en Anillo

En esta topología las terminales se conectan entre sí conformando un anillo, es decir, cada estación está conectada a la siguiente y la última a la primera. Cada estación tiene un receptor y un transmisor (que funciona como repetidor), pasando la señal a la siguiente estación del "anillo". La gran desventaja de esta topología es que si la red falla en uno de las terminales, o si falla una terminal en sí, se pierde la conexión para todos los demás. En la imagen se ilustra su funcionamiento:




## Redes en Árbol:

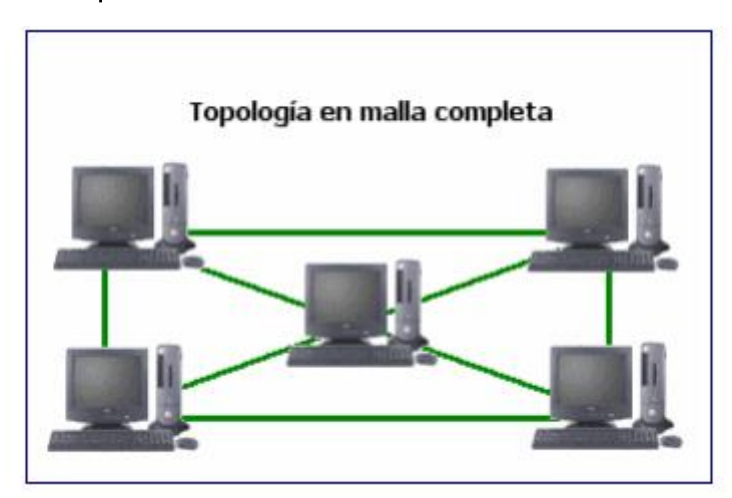
En este esquema la red se conecta en forma de árbol, se conectan independientemente cada equipo a un dispositivo que realiza la interconexión (un switch por ejemplo) y dicho dispositivo a su vez se conecta con otro de una jerarquía superior, al que pueden estar conectados otros que interconectan otras máquinas. La ventaja de este sistema es que si falla un nodo no se pierde la conexión hacia los demás nodos, y si falla por ejemplo un switch, no se perderá la conexión de toda la red. Se esquematiza a continuación:




## Red en Malla:

En esta topología cada nodo puede estar conectado a uno o más nodos de la red. Es decir, un mismo equipo puede estar conectado a otro equipo de la red o a más. Tiene

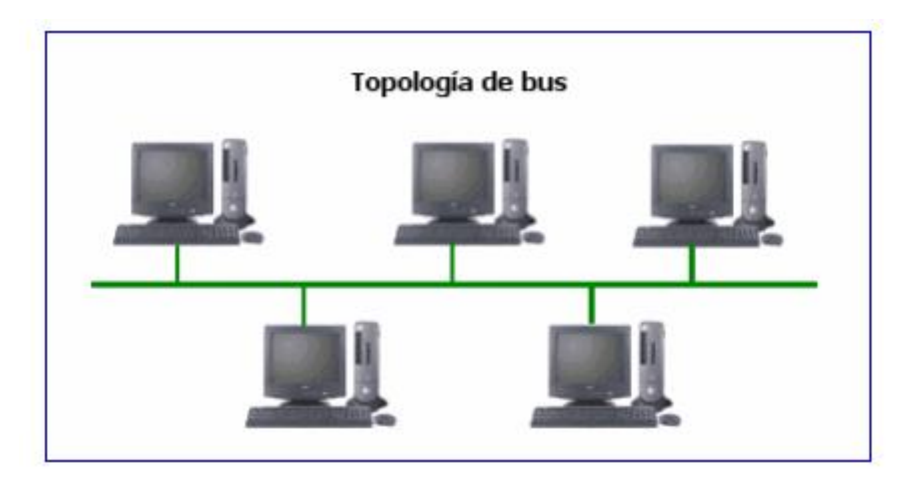
la ventaja de que si falla un terminal, la transferencia de datos puede tomar otro camino distinto (pasando por otros equipos). En un esquema completo (red malla completa) todos los equipos están conectados a su vez con todos los demás, evitando así la posibilidad de interrupción en las telecomunicaciones.




## Red en Bus

En esta topología todas las estaciones están conectadas a un único canal de comunicaciones por medio de unidades de interfaz y derivadoras. Las estaciones utilizan este canal para comunicarse con el resto.

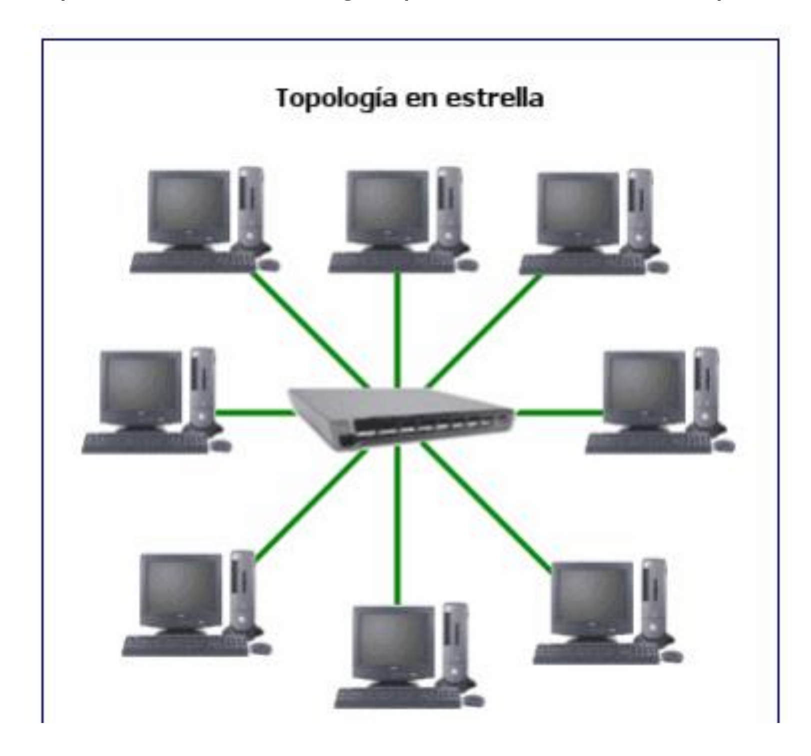
La topología en bus tiene todas las terminales conectadas a un mismo cable, lo que hace que todos los equipos estén conectados entre sí, pero la ruptura de dicho cable implicaría la caída completa de la red. Esta topología permite que todos los equipos puedan ver todas las señales de todos los demás dispositivos, lo que es ventajoso sólo si se desea que todos accedan a esa información, pero a menudo produce problemas de tráfico y colisiones de datos. Se puede utilizar en pequeñas redes domésticas conectando el cable a un hub o switch final en uno de los extremos.




## Red en Estrella:

Esta topología es bastante común y consta de que todas las terminales se conectan a un dispositivo central que se encarga de nuclear la red. Este dispositivo puede ser un hub, un switch o un router, y tiene la ventaja fundamental de que si falla un nodo

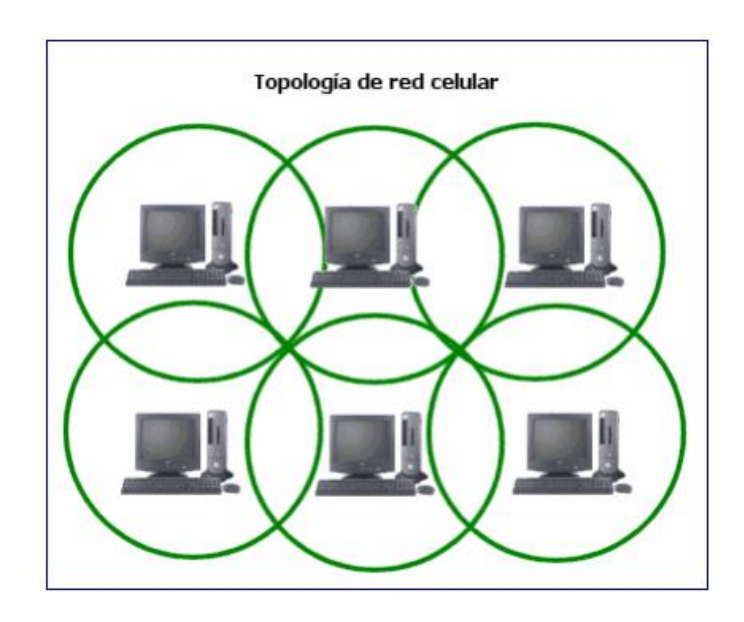
(una computadora) las demás pueden seguir conectadas entre sí. La conexión entre dispositivos es independiente, tiene la desventaja de que se utilizan más cables y el costo del cableado puede ser alto, además de que en caso de fallar el dispositivo central, entonces cae toda la red. La garantía de la integridad de los datos evitando colisiones depende de la tecnología que se utilice como dispositivo central.




## Red Celular:

La topología celular está compuesta por áreas de forma circular o hexagonal, cada una de las cuales tiene un nodo individual en el centro. La topología celular es un área geográfica dividida en regiones (las que denominamos, celdas) para los fines de la tecnología inalámbrica.

En esta tecnología no existen enlaces físicos; sino que sólo se transmiten los datos a través de ondas electromagnéticas. La ventaja obvia de una topología celular inalámbrica es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad. Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.




## Red Mixta:

Se le llama “red mixta” a una red donde coexisten varias topologías diferentes, puede ser una interred o simplemente una red diseñada de tal modo que se mezclan topologías.

*Imágenes extraídas de CSUDP*

# Clasificación de redes según su Alcance

## Redes de Área Personal (Personal Area Network)

Se le denomina redes PAN a aquellas redes cuya dimensión involucra el entorno de una persona, aproximadamente un metro cuadrado. Existen redes PAN por ejemplo establecidas dentro de los dispositivos de una persona cuando va escuchando música utilizando auriculares Bluetooth conectados a su teléfono celular (la red Bluetooth entre los auriculares y el teléfono conforman una PAN). Otro ejemplo de redes PAN, es en el equipamiento médico, donde a un paciente internado se le conectan dispositivos con sensores que miden sus funciones vitales. Dichos dispositivos se encuentran conectados en red para obtener esos datos provenientes de los sensores.

## Redes de Área Local (Local Area Network)

Las redes LAN, son redes de propiedad privada cuyo alcance se limita a un mismo edificio, como puede ser una oficina o un hogar. Se utilizan para interconectar computadoras u otros electrodomésticos con el fin de compartir recursos (como puede ser una impresora o el acceso a Internet). Cuando las empresas utilizan este tipo de redes, se las conoce como **redes empresariales**. A menudo se utilizan en restaurantes, cafeterías y lugares públicos empleando tecnologías de hardware inalámbricas, en estos casos, es cuando hablamos de redes **W-LAN**.

En el caso de las redes inalámbricas, los dispositivos que se conectan a través de Wi-Fi emplean protocolos de comunicación que permiten conectarse de manera inalámbrica a un enrutador central o Punto de Acceso (“Access Point” en Inglés, abreviado AP) quien transmite paquetes entre las computadoras inalámbricas y a su vez, al módem o dispositivo que conecta la red con internet, permitiendo el acceso de cada equipo conectado a la red global.

Las redes LAN, involucran un alcance que puede llegar hasta un kilómetro cuadrado de distancia.

## Redes de Área de Campus (CAN)

En muchas ocasiones, como en varios edificios vecinos, en universidades o en barcos comerciales se puede superar el área definida para las LAN, de un kilómetro. Sin embargo se hace necesario el establecimiento de una red veloz, estas son, las redes CAN.

A grandes rasgos, una red CAN es un conjunto de redes LAN interconectadas entre sí por un medio eficiente, que permite que todos los equipos se encuentren dentro de una misma red de mayor alcance.

## Redes de Área Metropolitana (MAN)

De mucho mayor alcance que las anteriores, las redes MAN pueden interconectar varias redes LAN en un área de hasta 50 kilómetros. Son típicamente utilizadas en ciudades para interconectar sucursales de una misma empresa, o en edificios distantes de un mismo ente público, empleando diversas tecnologías que permiten dicha conexión de manera rápida, como en la actualidad podrían ser WiMax o fibra óptica.

## Redes de Área Amplia (WAN)

Del Inglés “Wide Area Network” las redes de área amplia pueden cubrir distancias de cientos de kilómetros, permitiendo así la conexión entre ciudades distantes o incluso varios países. Estas redes pueden utilizar diferentes tipos de tecnologías para su implementación, dependiendo de las necesidades, se pueden emplear cables de fibra óptica o incluso satélites, para interconectar nodos distantes.

## Redes de Área de Almacenamiento (SAN)

Del Inglés “Storage Area Network”, es una red dedicada al almacenamiento que está vinculada a redes de comunicación de una compañía. Se emplean en empresas que trabajan con servidores, manejan una gran cantidad de datos y no quieren perder rendimiento. Los equipos conectados a una red SAN, además de contar con interfaces de red tradicionales, poseen una interfaz de red específica que se conecta a la SAN, el rendimiento de la red está directamente relacionado con el tipo de red que se utiliza, lo óptimo en la actualidad, es utilizar un canal de fibra óptica.

# Medios de Red

Un medio de red es la vía por la cual se transmiten los datos entre un emisor y un receptor dentro de cualquier red. Anteriormente, en el comienzo de este trabajo se habló de que un medio de red era el material por donde viajaban los datos que son transmitidos entre pares. No obstante, en este capítulo profundizaremos un poco en este aspecto y pasaremos a clasificar los tipos de medios existentes.

Para empezar, existen dos grandes clasificaciones:

- Medios de transmisión **guiados** o **alámbricos,** donde la señal viaja a través de cables o “alambres”, actualmente las tecnologías apuntan al uso de cables de cobre o fibra óptica, donde se transmite luz dentro del cable.

- Medios de transmisión **no guiados** o **inalámbricos**, para estos casos, se utiliza el aire como medio de transmisión, a través de microondas, radiofrecuencias o luz (por ejemplo en el caso de la comunicación por infrarrojos).

## Medios Guiados: Tipos de cable

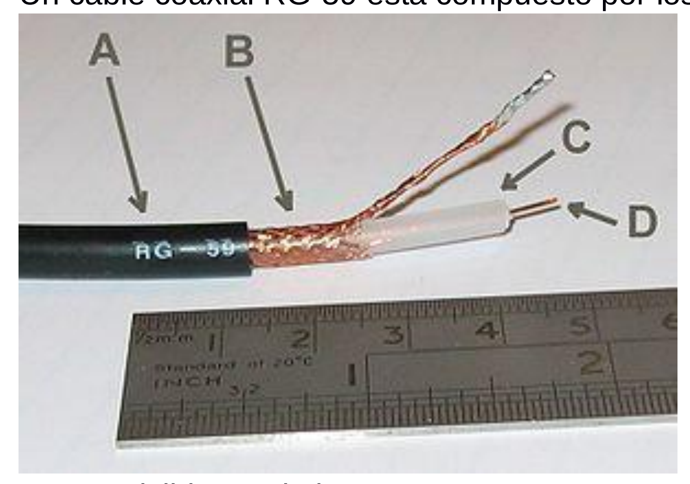
Detallaremos brevemente sobre los tipos de cables más utilizados en redes computacionales:

- Cable coaxial

  Este tipo de cable fue creado en la década de los años 1930s, y se utiliza para la transmisión de señales eléctricas de alta frecuencia que posee dos conductos concéntricos, uno interior que se encarga de transportar la información y una malla exterior o protectora que se encarga de referencia de tierra y retorno de corrientes.

  Es típicamente usado para redes de cable televisivo, pero también se utilizó para redes de computadoras.

Un cable coaxial RG-59 está compuesto por los siguientes componentes:




*Partes visibles en la imagen:*

A) *Cubierta protectora de plástico (Elastómetro termoplástico)*
B) *Malla de cobre (conductor blindado de tranza de aluminio recubierto de cobre)*
C) *Aislante (dieléctrico de espuma)*

*D) Conductor central o núcleo de cobre (acero recubierto de cobre)*
*Imagen e información detallada obtenida de Wikipedia*

- Cable de Par Trenzado:
  Este tipo de cable es de los más comunes en redes domésticas, de oficina y otras redes cableadas, consta de 8 hilos aislados entre sí, trenzados de dos en dos. Esto se realiza para cancelar las ondas que pueden llegar a transmitirse entre sí, disminuyendo la posible interferencia producida por los cables y permitiendo así una mejor transmisión de datos. Para proteger los cables de posibles interferencias electromagnéticas exteriores, algunos cables par trenzado incluyen blindaje aislante.

### Clasificación de cables par trenzado según blindaje:

Antes de desarrollar una posible clasificación vamos a desarrollar brevemente un concepto proveniente de la electrónica, y es el de **impedancia**, que es la medida de oposición que presenta un circuito a una corriente cuando se aplica una trensión. Refiere a algo similar a la resistencia, pero se extiende a circuitos de corriente alterna (AC), siendo que cuando se está trabajando con corriente continua (CC), la impedancia es igual a la resistencia. La impedancia a diferencia de la resistencia, toma en cuenta la fase (diferencia de tiempo) de las ondas, y no sólo su magnitud, por lo que a diferencia de la resistencia, la impedancia cambia al cambiar dicha frecuencia.

En su fórmula, la impedancia (Z) está determinado por el cociente entre la tensión y la intensidad (V / I), del mismo modo que se calcula la resistencia, la cual no toma en cuenta las fases.

Existe cable par trenzado blindado y no blindado, a saber:

- Unshielded Twisted Pair / UTP (Par Trenzado sin Blindaje): Son cables de pares trenzados sin blindaje externo, ampliamente utilizados por su fácil uso y bajo costo, sin embargo son vulnerables a interferencias electromagnéticas que hacen que la señal pueda perderse a medida que se aumenta la distancia. Estos cables son propicios para transmisión a corta distancia (por ejemplo en redes LAN domésticas o de oficina) pero no son aconsejables para redes más amplias, ya que sin recuperación de señal tienen poco alcance. Poseen una impedancia de 100 ohmios.
- Shielded Twisted Pair / STP (Par Trenzado Blindado):
  Son cables donde los pares trenzados se encuentran aislados por una cubierta protectora, con un número específico de trenzas por hilo. STP hace referencia a la cantidad de aislamiento alrededor de un conjunto de cables y por ende su inmunidad ante el ruido, poseen una impedancia de 150 ohmios.



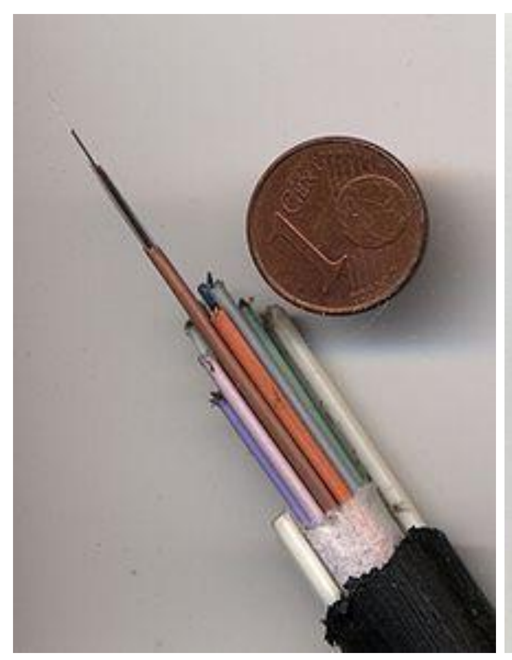
*Imagen de un cable STP, tomada de* *[Wikipedia]*

- Cables de fibra óptica:

  Los cables de fibra óptica son la tendencia de la actualidad en redes de computadoras y en telecomunicaciones en general, están marcando un gran cambio en el presente, ofreciendo grandes ventajas frente a tecnologías anteriores, y podría inferirse que van a quedarse con nosotros por varios años a futuro debido a sus grandes prestaciones. Los cables de fibra óptica están conformados por un grupo de fibras que transmiten señales luminosas, las fibras comparten su espacio con hiladuras de aramida que le confieren la necesaria resistencia a la tracción.

  Las ventajas que ofrecen los cables de fibra óptica frente a tecnologías anteriores radica así no sólo en la velocidad de transferencia de datos (gracias a que la luz se propaga a través de los cables de fibra a enorme velocidad) sino también en la distancia que pueden llegar a cubrir sin necesidad de reconstruir la señal. Un cable de 8 fibras ópticas tiene un tamaño mucho más pequeño que los cables par trenzado usados normalmente, pero puede soportar las mismas comunicaciones que 60 cables de 1623 pares de cobre o 4 cables coaxiales de 8 tubos, todo eso con una distancia entre repetidores mucho mayor. Una bobina de cables de fibra óptica de 8 fibras pesa aproximadamente 30 Kg por cada kilómetro a cubrir, lo que permite efectuar tendidos de 2 a 4 km a la vez, mientras que con un cable de cobre no sería viable un tendido de más de 200 a 250 metros cada tramo.

  Cabe en esta instancia imaginar, la amplia ventaja que ofrecen los tendidos de fibra óptica en lo que refiere a practicidad, pero brevemente compararemos las tecnologías posibles en lo que refiere a velocidad, frecuencia y la distancia máxima que puede recorrer una señal sin perderse, respecto de las tecnologías más antiguas.




*A la izquierda puede verse una sección de un cable de fibra óptica, a la derecha unos conectores de cable de fibra óptica tipo ST. Ambas imágenes, obtenidas de [Wikipedia](Wikipedia)*

### Clasificación de cables de fibra óptica:

Las diferentes trayectorias que puede recorrer un haz de luz dentro de un cable de fibra óptica es lo que se conoce como **modo de propagación,** y según esta clasificación existen fibras multimodo y monomodo.

- Fibra óptica multimodo: En este tipo de comunicación, un haz de luz puede transmitirse a través de más de mil modos o caminos diferentes, lo que quiere decir que no todos los haces llegan a la misma vez, es mucho más barato que el sistema monomodo, pero puede cubrir áreas de hasta 2 kilómetros aproximadamente (ideales para redes de área de campus).

- Fibra óptica monomodo: En este tipo de fibra óptica, la transmisión se hace a través de un solo modo de luz. Esto se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño que sólo permita un modo de propagación (esto es, llevarlo a 9,3 a 10 micrones -1 micrón es igual a una milésima parte de un milímetro-). Su transmisión es siempre paralela al eje de la fibra, las fibras monomodo permiten cubrir distancias mucho mayores que las multimodo (hasta 400 km a través de un láser de alta intesidad) a una velocidad de 10 Gbits/s.

## Comparativa de velocidad, frecuencia y distancia en medios guiados

Para poder resumir el tema de los posibles medios de red, vamos a concluir con una tabla comparativa que permita visualizar fácilmente las mayores diferencias que ofrecen las diferentes tecnologías en medios de redes. Compararemos las tecnologías

más comunes en la actualidad, y veremos cómo, sería esperable que en un futuro no muy lejano, los cables de fibra óptica se vayan convirtiendo cada vez más en un estándar, y las tecnologías anteriores queden absolutamente obsoletas.

Cabe destacar, que en varios países las redes de fibra óptica se han convertido ya en el estándar (aplicando tecnologías FTTx) y los cables de cobre sólo están siendo usados para redes en los interiores de los edificios o entre los equipos del hogar (debido al costo de tener equipos conectados entre sí por fibra óptica, y la menor posibilidad de pérdida de información que hay en distancias chicas, es entendible que dentro de los hogares se sigan utilizando tecnologías con cable par trenzado, por ejemplo).

| **Tipo de Cable** | Velocidad de transferencia de datos | Ancho de banda utilizado por la señal | Distancia máxima que pueden cubrir sin reconstruir la señal |
|---|---|---|---|
| UTP Categoría 3 | 4 Mbps | 16 MHz | 100m |
| UTP Categoría 4 | 16 Mbps | 20 MHz | 100m |
| UTP Categoría 5 | 100 Mbps | 100 MHz | 100m |
| UTP Categoría 5e | 1000 Mbps | 100 MHz | 100m |
| UTP Categoría 6 | 1 Gbps | 250 MHz | 100m |
| UTP Categoría 6e | 10 Gbps | Inicial 250 MHz – 500 MHz | 100m |
| U/FTP Categoría 7 | 10 Gbps | 600 MHz | 100m |
| Fibra Óptica OM1 | Dependiendo de la distancia, 100 Mbps hasta 1km, 1Gbps hasta 275m, 10Gbps hasta 33m | 250 a 500 MHz por kilómetro | 33 a 1000m |
| Fibra Óptica OM2 | 100 Mbps hasta 2km, 1Gbps hasta 550m, 10 Gbps hasta 82m | 500 MHz por kilómetro | 82 a 2000m |
| Fibra Óptica OM3 | 100Mbps hasta 2km, 1Gbps hasta 550m, 10Gbps hasta 300m, 40/100 Gbps hasta 100m. | 1500 a 2000 MHz por kilómetro | 100 a 2000m |
| Fibra Óptica OM4 | 100Mbps hasta 2km, 1Gbps hasta 1km, 10Gbps hasta 400m, 100 Gbps hasta 150m. | 3500 a 4700 MHz | 100 a 2000m |

Como puede observarse, los cables de fibra óptica **multimodo** son clasificados también **según su núcleo y diámetro de revestimiento** en tipos OM1, OM2, OM3 y OM4. Para los cables OM1 y OM2 usualmente se recomienda el color naranja, mientras que para las OM3 y OM4 por lo general se utilizan cables en color aqua.

## Ejercicios para evaluar unidad de protocolos y medios de redes

En principio se habló desde un punto de vista muy teórico, del concepto que vamos a trabajar sobre comunicación, sobre redes canales de comunicación, capacidad de los canales, etc. Luego, pasamos a adentrarnos en la arquitectura de redes de computadoras, viendo algunos posibles criterios de clasificación (por su topología y alcance, pero se invita al lector a investigar otros), también se habló de protocolos de comunicación y modelos de referencia de arquitectura de redes, en concreto, OSI y TCP/IP.

Por último, hablamos de medios de redes, lo que comprende al medio físico por el cual se realiza la comunicación, este punto es muy importante, ya que de él depende la velocidad en la transferencia de bits según el medio utilizado, pudimos ejemplificar y comparar los diferentes medios teniendo en cuenta las tecnologías que conocemos actualmente.

A modo de estar seguros de que los conceptos anteriores esten bien comprendidos, y podamos continuar a adentrarnos en las diferentes capas de red y sus protocolos, invitamos al lector a realizar algunas preguntas, como ejercicio mental puede intentar responderlas sin mirar en otras partes del texto (ni ayuda de Internet), y luego buscar en el texto o en otras fuentes fiables, y comparar la idea que tenía con la que se está manejando. Es simplemente una idea de autoevaluación. En fin, vamos a ello:

1) ¿A qué le llamamos “arquitectura de red”?
2) ¿Cómo pueden clasificarse las redes de computadoras según su extensión?
3) ¿Cuáles son las capas del modelo OSI? ¿Puede explicar muy brevemente para qué sirve cada una?
4) ¿Qué diferencia hay entre medios de red guiados y no guiados?
5) ¿Qué es un cable UTP? ¿En qué se diferencia con un STP?
6) Explique las diferencias prácticas que existen entre la utilización de cableado de cobre contra el uso de cableado de fibra óptica en una red.

# Cableado Estructurado

Continuando la temática que se desarrollaba anteriormente sobre medios de redes, y teniendo en cuenta el énfasis que se la ha dado a los medios guiados, vamos a dedicar un espacio ahora a trabajar un tema relacionado con el diseño interno de una red dentro de un edificio, y cómo podría organizarse el cableado dentro de él.

Imaginemos que para instalar una pequeña red doméstica en nuestra casa, interconectando un equipo que está en el living con otros dos que están cada uno en un dormitorio, no hay grandes complicaciones; podemos instalar un switch en un espacio que nos guste, y a él traer el cableado de cada computadora usando simplemente cable UTP, amurándolo prolijamente a la pared usando ductos. El modem de conexión ADSL de nuestra proveedora lo podemos conectar también al switch, y así nuestro dispositivo retransmitirá la conexión a Internet a todos los otros conectados. Fácil, ¿No? Este esquema es válido para un hogar, pero, ¿Cómo organizaríamos una red LAN para un edificio de diez pisos con varias oficinas en cada uno?

Seguramente si no seguimos algún estándar concreto para diseñar el sistema de la red, podríamos chocarnos con una enorme dificultad, ya que la cantidad de equipos a interconectar harían que la red se vuelva extremadamente compleja de crear y mantener.

Lo cierto es que hasta 1985 no existía un estándar a seguir, el diseñador de una red tenía que idear el esquema de conexión dependiendo de los requerimientos de cada situación particular. En 1985, la CCIA (Computer Communications Industry Association) solicitó a la EIA (Electronic Indistry Alliance) realizar un estándar de sistemas de cableado. La EIA ha desarrollado hasta el día de hoy, un conjunto de recomendaciones o estándares para definir el diseño de redes para industrias o residencias, elaborando un conjunto de normas conocidas en el ámbito de las redes, la que se ocupa de definir espacios y canalizaciones para edificios comerciales, es la norma ANSI/TIA/EIA-569, y de acuerdo a ella es que trabajaremos en esta etapa del trabajo.

**El cableado estructurado,** es entonces la manera en la cual se organiza el cableado de una red en el interior de un edificio, a menudo haciendo uso de cables par trenzado, tanto blindados como no blindados.

Existen 3 aspectos fundamentales sobre los cuales se funda la norma ANSI/TIA/EIA-569, que se encarga de definir “Espacios y Canalizaciones para Edificios Comerciales” a saber:

- *Los edificios son dinámicos. Durante la existencia de un edificio, las remodelaciones son comunes, y deben ser tenidas en cuentas desde el momento del diseño. Este estándar reconoce que el cambio ocurre y lo tiene en cuenta en sus recomendaciones para el diseño de las canalizaciones de telecomunicaciones.*
- *Los sistemas de telecomunicaciones son dinámicos. Durante la existencia de un edificio, las tecnologías y los equipos de telecomunicaciones pueden cambiar dramáticamente. Este estándar reconoce este hecho siendo tan independiente como sea posible de proveedores y tecnologías de equipo.*
- *Telecomunicaciones es más que “voz y datos”. El concepto de Telecomunicaciones también incorpora otros sistemas tales como control ambiental, seguridad, audio,*

*televisión, alarmas y sonido. De hecho, telecomunicaciones incorpora todos los sistemas de “bajo voltaje” que transportan información en los edificios.*
(Joskowicz, 2006)

Para un funcionamiento óptimo de la estructura de telecomunicaciones de un edificio, escalable y mantenible en el paso del tiempo, teniendo en cuenta los puntos antes mencionados, , es necesario que el diseño de las telecomunicaciones se desarrolle previamente al diseño arquitectónico del edificio. El estándar antes mencionado identifica seis componentes en la infraestructura de telecomunicaciones edilicia:

- Instalaciones de Entrada
- Sala de Equipos
- Canalizaciones de “Montantes” (“Back-bone”) ·
- Armarios de Telecomunicaciones
- Canalizaciones horizontales
- Áreas de trabajo

En la imagen a continuación, se ilustra un esquema relativamente completo, del cableado estructurado en un edificio de varios pisos:

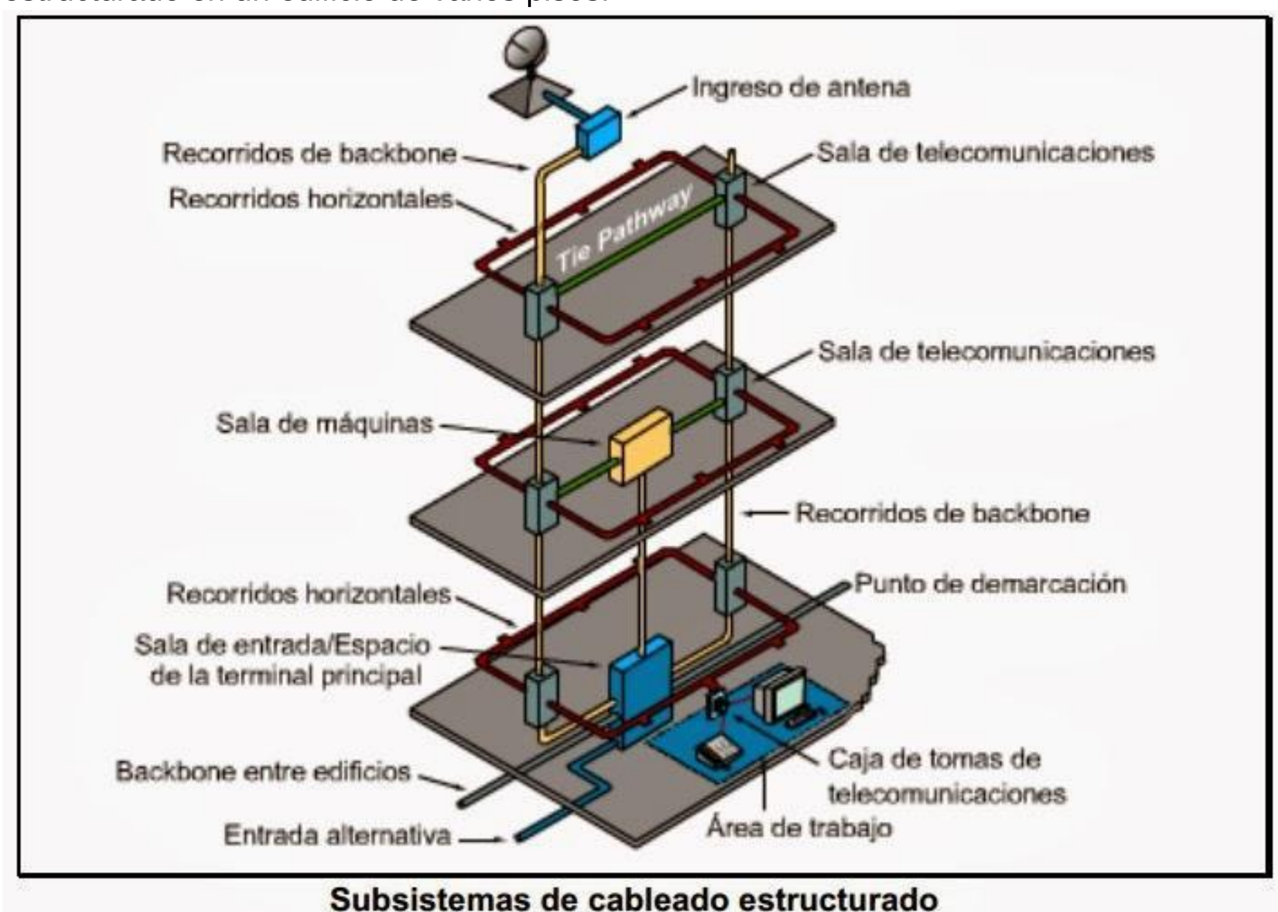



*Imagen extraída del blog Conocimientos de Hoy*

## Subsistemas del Cableado estructurado

Existen en total siete subsistemas relacionados con el Cableado Estructurado, coinciden básicamente con los componentes citados anteriormente, pero al tratarse de partes con determinada funcionalidad bien definida y constituidos por equipamiento diferente, podemos diferenciar subsistemas distintos y contabilizar un total de siete. Cada uno de ellos se encarga de cubrir funciones determinadas para proveer servicios de datos o voz en toda la planta de cables. A continuación detallaremos más en profundidad cada uno de ellos.

### Punto de Demarcación (DEMARC)

Es el punto donde se conecta la red telefónica proveída por la compañía proveedora de servicios con la red del consumidor, es decir, la del edificio. Es en ese punto donde se conecta el cableado externo con las instalaciones de entrada del edificio. En la imagen que puede apreciarse debajo, se ven dos puntos de demarcación en un hogar canadiense construido en 1945, a la izquierda uno antiguo y a la derecha uno moderno, en el moderno se encuentra conectado un filtro DSL.

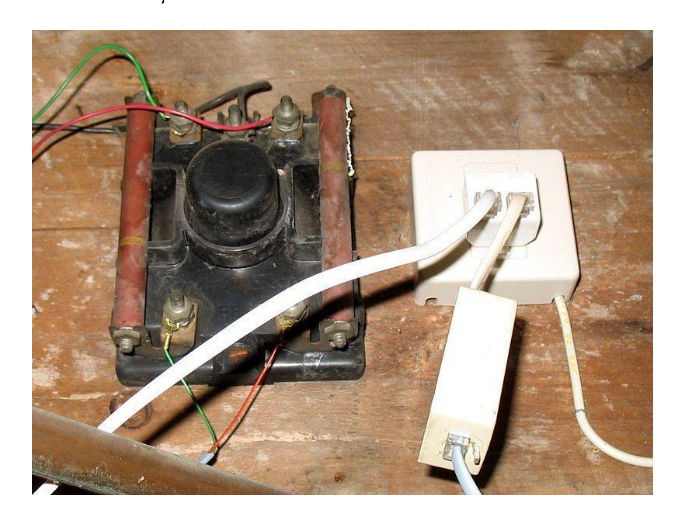


*Imagen extraída de Wikipedia*

### Instalación de entrada (EF)

Las instalaciones de entrada (EF) es el punto donde el cableado externo hace interfaz con el cableado dorsal (backbone) del edificio, consiste en la entrada de los servicios de telecomunicaciones al edificio (acometidas), incluyendo el punto de entrada a través de la pared y hasta el cuarto o espacio de entrada.

Es el lugar en el que ingresan los servicios de telecomunicaciones al edificio y/o donde llegan las canalizaciones de interconexión con otros edificios de la misma corporación (por ejemplo, si se trata de un “campus”).

### Cableado Dorsal (Backbone)

Permite la intercomunicación entre el gabinete o rack de telecomunicaciones, los cuartos de telecomunicaciones y los servicios de la entrada. Está compuesto por cables

de conexión vertical entre pisos (conocidos como risers), el cableado entre el cuarto de equipos y el cable de entrada a los servicios del edificio, y el cableado entre edificios.

### Cuarto de Equipos

Se define como el espacio dónde se ubican los equipos de telecomunicaciones comunes al edificio. Estos equipos pueden incluir centrales telefónicas (PBX), equipos informáticos (servidores, switches, routers, etc), Centrales de video, etc. Sólo se admiten equipos directamente relacionados con los sistemas de telecomunicaciones.

### Gabinete, Armario o Rack de Comunicaciones

Se define como el punto de transición entre las canalizaciones verticales (el backbone) y las canalizaciones de distribución horizontal. Estos armarios o salas generalmente contienen puntos de terminación e interconexión de cableado, equipamiento de control y equipamiento de telecomunicaciones (típicamente equipos "activos" de datos, como por ejemplo hubs o switches). No se recomienda compartir el armario de telecomunicaciones con equipamiento de energía.

La ubicación ideal de los armarios de telecomunicaciones es en el centro del área a la que deben prestar servicio. Se recomienda disponer de por lo menos un armario de telecomunicaciones por piso; en los casos donde el área a servir supere los 1000 metros cuadrados se recomienda otro armario o sala por cada 1000 metros cuadrados de área utilizable. Adicionalmente, en los casos donde la distancia de las canalizaciones de distribución horizontal desde el armario de telecomunicaciones hasta las áreas de trabajo supere los 90 metros, debe proveerse de otro armario, ya que esa distancia no puede superar los 90m.

### Cableado Horizontal

Son las canalizaciones que distribuyen los cables desde la sala de comunicaciones hasta los equipos de trabajo. Consta del cableado propiamente dicho, los enchufes de telecomunicaciones, las terminaciones de los cables (asignaciones de guías de conector modular RJ-45) y las conexiones de transición.

Existen tres tipos de medios reconocidos para el cableado horizontal, que en ninguno de los casos deben superar la distancia de 90 metros; el cable UTP, el STP y el cable de fibra óptica.

### Área de Trabajo:

Los componentes del área de trabajo se extienden desde el enchufe de telecomunicaciones a los dispositivos o estaciones de trabajo.

Los componentes del área de trabajo son los siguientes:

- Dispositivos: computadoras, terminales, teléfonos, etc.
- Cables de parcheo: cables modulares, cables adaptadores/conversores, jumpers de fibra, etc.
- Adaptadores – Aquellos que sean externos al enchufe de telecomununicaciones.

## Cableado Horizontal y Áreas de Trabajo: Consideraciones especiales

Dentro de los subsistemas existentes para la disposición del cableado estructurado, aquellas instalaciones horizontales, es decir, desde la conexión al backbone con los equipos terminales de los usuarios, son las que suelen requerir cambios con mayor frecuencia y deben estar preparadas para una adecuada mantenibilidad y futuras modificaciones. Imaginemos una compañía con un edificio de varios pisos, ¿Es común que en uno de los pisos se realicen cambios en el mobiliario, verdad?

Imaginemos un gran edificio de una compañía de correos, donde en planta baja se manejan las áreas de atención al cliente y depósito de paquetes, en el primer piso está la parte administrativa-contable, en el segundo se encuentran las áreas de soporte informático y electrónica, en el tercero funciona el call center y en los demás, quedan a imaginación del lector. Supongamos que todo el sector de los administrativos se desea cambiar, ya que la compañía contaba con 10 áreas de trabajo pero se suman 2 empleados nuevos, se requiere para cada uno un área de trabajo diferente, además se desea cambiar la distribución de las áreas para que exista mejor movilidad dentro de la sala y los empleados tengan mayor facilidad para trasladarse entre oficinas y realizarse consultas entre colegas. ¿No implicaría estos cambios, modificaciones en la instalación de la red, también? ¿No sería deseable que éstas modificaciones requieran del menor gasto posible y que no afecten a otros pisos?

### Oficina Abierta

La Oficina Abierta (del Inglés “Open Office”) es un concepto que refiere a ambientes donde la movilidad del personal es muy grande y requiere de soluciones rápidas para reorganizaciones departamentales o equipos de trabajo que en esencia requerirían de un gasto muy grande por concepto de recableados.

El cableado horizontal consiste en tramos “rígidos” de cable , que comienzan en los armarios de telecomunicaciones y terminan en las áreas de trabajo, estos tramos decimos que son “rígidos” porque no podemos moverlos a conveniencia sin implicar grandes costos. Los puntos “flexibles” existen únicamente dentro de los armarios de telecomunicaciones (dónde puede interconectarse cualquier área de trabajo a cualquier equipo o cable de backbone) y en las propias áreas de trabajo (dónde mediante patch-cords pueden conectarse los PCs, teléfonos, impresoras, etc.). Combinado al mobiliario modular existen soluciones para garantizar mayor flexibilidad ante los cambios y movilidad entre oficinas.

En concreto, las dos soluciones conocidas son las salidas de comunicaciones multiusuario (MUTOA) y los puntos de consolidación (CP). Se puede optar por cualquiera de estas dos opciones válidas, dependiendo de algunos detalles, como la cantidad de usuarios del área, la distancia que tendrán los cables hasta las salas de telecomunicaciones, y la misma distribución de la sala.

### MUTOA (Multiuser Telecommunications Outlet Assembly)

Los Ensambles de Salidas de Telecomunicaciones Multiusuario (en adelante, MUTOA) son una posible configuración para eliminar el problema de la movilidad de un ambiente de trabajo. Es un equipo que permite que los usuarios se trasladen y agreguen

equipos, y que realicen cambios en la distribución de los muebles modulares sin volver a tender el cableado. Los cables de conexión se pueden tender directamente desde el MUTOA hasta el equipo del área de trabajo. El MUTOA, no puede ser instalado sobre el techo ni debajo del piso de acceso; tampoco se admite su montaje sobre muebles a no ser que éstos se encuentren instalados de forma permanente al edificio.

Las recomendaciones para instalar los MUTOA están definidas en el estándar TIA/EIA-568-B.1 y se incluyen las siguientes pautas:

- Se necesita al menos un MUTOA por cada grupo de muebles
- Cada MUTOA puede prestar servicio hasta a 12 áreas de trabajo.
- Los cables de conexión de las áreas de trabajo se deben rotular en ambos extremos con identificaciones exclusivas.
- La longitud máxima del cable de conexión es de 22 metros.

## Punto de Consolidación (CP)

Son configuraciones que ofrecen un acceso limitado a las conexiones del área, En este esquema, los equipos de las áreas de trabajo no se conectan a un CP como se hace con los MUTOAs, las estaciones se conectan a un toma, que a su vez se conecta a un CP.

Es el estándar TIA/EIA-569 el que define las consideraciones para instalar los CP, y establece que:

- Se necesita como mínimo un CP para cada grupo de muebles.
- Cada CP puede prestar servicio a un máximo de 12 áreas de trabajo.
- La longitud máxima del cable de conexión es de 5 metros.

Tanto en los CP como en los MUTOA, el estándar TIA/EIA 568-B.1 recomienda una separación de al menos 15 metros por equipo entre la sala o rack de Telecomunicaciones y el CP o los MUTOA.

En la imagen a continuación pueden apreciarse las diferencias en la instalación de los dos esquemas:

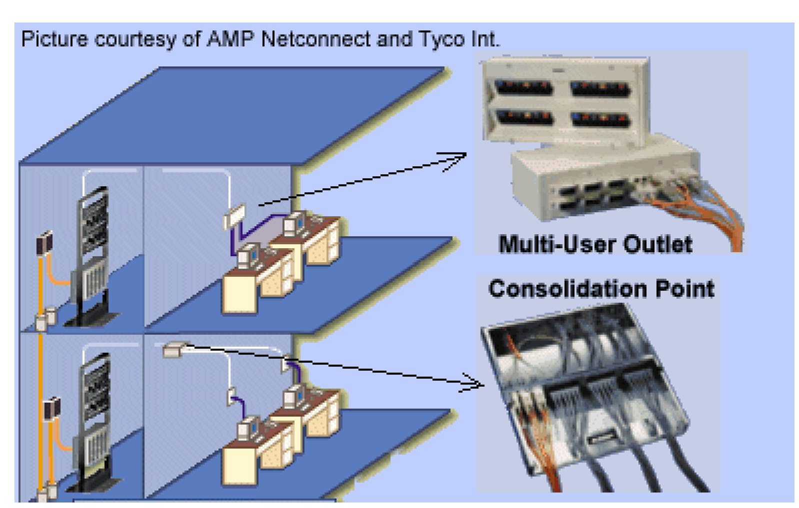



*Imagen extraída del sitio HowToDoIt*

## Normas y Códigos para el Cableado - Características Mecánicas

- *El diámetro de cada cable no puede superar los 1.22 mm*
- *Los cables deben ser de 4 pares únicamente.*
- *No se admite para el cableado horizontal cables de más o menos pares. (Notar que si se admiten cables "multipares" para los backbones)*
- *Los colores de los cables deben ser los siguientes:*

*Par 1: Azul-Blanco , Azul (W-BL)(BL)*
*Par 2: Naranja-Blanco , Naranja (W-O)(O)*
*Par 3: Verde-Blanco , Verde (W-G)(G)*
*Par4: Marrón-Blanco , Marrón (W-BR)(BR)*




- *El diámetro completo del cable debe ser menor a 6.35mm*
- *Debe admitir una tensión de 400 N*
- *Deben permitir un radio de curvatura de 25.4 mm (1") sin que los forros de los cables sufran ningún deterioro*

## Características Eléctricas para el cableado Horizontal

- *La resistencia "en continua" de cada conductor no puede exceder los 9.38 Ω por cada 100 m a 20 ºC.*
- *La diferencia de resistencias entre dos conductores del mismo par no puede superar en ningún caso un 5%*
- *La capacitancia mutua de cualquier par de cables, medida a 1 kHz no puede exceder los 6.6 nF en 100 m de cable para Categoría 3 y 5.6 nF en 100 m de cable para Categoría 5e. La capacitancia desbalanceada, entre cualquier cable y tierra , medida a 1 kHz, no puede exceder los 330 pF en 100 m de cable.*
- *La impedancia característica del cable debe ser de 100 Ω +/- 15% en el rango de las frecuencias de la categoría del cable*

Información extraída de Joskowicz (2013)

## Proceso de Instalación del Cableado estructurado (fases)

Para llevar a cabo un proyecto de instalación de un sistema de cableado estructurado como del que se hablaba anteriormente, es necesario realizar una serie de fases. La empresa encargada de armar el cableado debe tener en cuenta las siguientes etapas:

1. Preventa / Venta (Definición del proyecto y el presupuesto)
2. Obra gruesa (Tendido y ruteo de cables)
3. Terminación (Ajustes o recortes, y conexiones)
4. Finalización (Pruebas, diagnóstico de fallas y certificación)
5. Asistencia al cliente

Veamos brevemente cada una de estas etapas por separado:

### *Preventa y Venta*

Esta etapa está constituida por las siguientes tareas:

- *Clasificación de las Solicitudes de Propuesta* (RFP, del Inglés “Request For Proposals) o solicitudes de presupuesto (RFQ, del inglés “Request For Quotation”), que son documentos donde se definen en detalle las necesidades del cliente o el proyecto a llevar a cabo. En respuesta a un RFP, es imprescindible que participen todas las personas de la empresa de cableado, que se lean y entiendan todos los aspectos.
- *Reunión previa a la oferta*
  Esta reunión realizada con el contratista debe aclararle al mismo todos los aspectos referentes a su proyecto, de modo que se le permita brindarle una imagen clara del presupuesto con el que deberá contar. Para brindar una respuesta a las RFP, se debe contemplar todos sus requisitos. En la reunión es importante además, brindarle una descripción general de la empresa (o las empresas) que realizarán las instalaciones, como también de su trayectoria y de proyectos previos que hayan realizado. Se debe especificar los materiales, la mano de obra, los posibles subcontratistas y el margen de utilidades a emplear (esto último es, un aumento al precio final para obtener un margen de ganancia).
- Recopilación de los requisitos
- Planificación
- Cálculo de Costos de Mano de Obra
- Elaboración de propuesta u oferta
- Redacción del contrato y negociaciones.

### *Obra Gruesa (Tendido y Ruteo de Cables)*

- Esta obra consiste en el tendido de los cables que van a comprender hasta las áreas de trabajo.
- Cada uno de los cables colocados a la sala de comunicaciones van rotulados de ambos lados, de modo de comprender qué están interconectando.
- Los proyectos de instalación del cableado varían según si se trabaja en nuevos edificios en construcción, en edificios antiguos sin uso o en edificios antiguos actualmente en uso.
- En el caso de trabajar en edificios antiguos, el instalador del cable debe identificar los circuitos activos para no quitarlos accidentalmente, quitar el cable abandonado para crear un nuevo cableado y planificar el corte de servicio eléctrico y/o telefónico mientras se llevan a cabo las obras. Esto requiere notificar a los inquilinos del edificio cuando ocurra.
- Requiere de herramientas como carretes de cable, árbol de cables (sostenedor de carretes pequeños), gatos elevadores para cable, rodillos de carrete, ruedas de giro, poleas, canaletas.
- Comprende la instalación de cableado vertical y el cableado horizontal.

### *Terminación*

- Las tareas principales durante esta etapa son: la administración de los cables y la conexión de los alambres. La etapa de terminaciones también puede perturbar el trabajo del cliente. Es habitual que sea necesario mover escritorios o muebles para tener acceso a los tomas. Esta etapa debe realizarse en el mayor silencio posible, y debe limpiar todo de manera adecuada cuando estén instaladas las tomas.

### *Finalización (Pruebas de Cables y certificación)*

- Las tareas principales durante la etapa de finalización son: prueba de los cables, diagnóstico de fallas y certificación. Aunque los cables de voz no requieren de ser certificados, se debe evaluar su continuidad y el mapeo del cableado.
- Los tipos de pruebas que se deben realizar a los cables UTP son:

*Mapa del Cableado*

La prueba de Mapa de cableado requiere comprobar para cada uno de los ocho conductores del cable que existe continuidad en todos ellos y que la longitud no supere lo indicado en la norma (cables para enlace de canales de 90 metros o enlaces permanentes de 100 metros). Para esto se requiere de un analizador de cable DTX 1800 como de su unidad remota. El mismo permite comprobar la continuidad en cada cable y la longitud, y establecer si el cableado pasó o no la prueba. Para eso se conecta el analizador en una de las puntas del cable a testear y la unidad remota en la otra, y el mismo permite analizar cada uno de los hilos del cable.

*Longitud del Cable*

De la manera explicada anteriormente, se puede realizar prueba de mapa del cableado en cuanto a continuidad de los cables y también de longitud de cada par de cables. Para ver una guía de cómo realizar estas pruebas paso por paso, se recomienda visitar la web de GonzaloNazareno - Mapa de Cableado

*Pérdida de Señal debido a Atenuación*

La atenuación en un canal de transmisión es la diferencia de potencias entre la señal inyectada a la entrada y la señal obtenida a la salida del canal. Los cables UTP son de hecho canales de transmisión, y por lo tanto, la potencia de la señal al final del cable (potencia recibida) será menor a la potencia transmitida originalmente.
Una prueba de atenuación tendrá como resultado un valor en Dbm (decibeles por metro de cable) que debería ser negativo, ya que debido al ruido, el canal no sufrirá amplificación sino que será atenuado en cada metro de cable. Cuanto menos negativo sea ese valor (menor atenuación), mejor será la medida del cable. Debemos recordar que medimos en Decibeles, que son unidades logarítmicas, por lo cual los valores no son directamente escalonados, ya que el decibel es una magnitud logarítmica que simplemente divide el cambio que muestra un Bel, donde cada Bel representa un cambio de diez veces en relación a la magnitud de referencia.

En el cable par trenzado, cada 6Db, tenemos un cambio del doble en la amplitud de la señal. Una atenuación de -6Db implica una atenuación donde la señal original se reduce a

la mitad. Esta medida además, es proporcional a la reducción del cable, es decir, la atenuación a 50m debe ser la mitad, de la atenuación a 100m.

*Crosstalk*

Near End Cross Talk o en español, “Diafonía de Extremo Cercano”. Mide la Diafonía existente entre un par transmisor y un par adyacente dentro del mismo cable. La medición se realiza en ambos extremos, para todas las combinaciones posibles, arrojando 12 resultados.(Se produce diafonia o crosstalk, cuando parte de las señales presentes en un extremo del cable, llamado perturbador, aparece en el otro, considerado perturbado. La herramienta de prueba mide la interferencia aplicando una señal de prueba a un par de cables y midiendo la amplitud de las señales de interferencia que se reciben en el otro par de cables. El valor de la interferencia se calcula como la diferencia de amplitud entre la señal de prueba y la señal de interferencia al medirse desde el mismo extremo del cable. Esta medida se expresa en decibelios, los valores más altos de NEXT corresponden a menos interferencia y un mejor rendimiento del cable. El origen de los errores puede ser cables defectuosos, demasiados conectores, destrenzado en las terminaciones, pares divididos, conectores de baja calidad, etc.

Para profundizar y ver cómo se realizan las pruebas, se recomienda consultar el artículo enlazado en el sitio web de GonzaloNazareno - Certificación en Cobre.

### *Asistencia al Cliente*

- La última etapa del proyecto se centra en la satisfacción del cliente. En esta etapa, se realiza una inspección de la red con el cliente y se le presentan los resultados formales de las pruebas y otra documentación, como los dibujos de la instalación terminada. El cliente puede aprobar el proyecto si está satisfecho. Luego la compañía de instalación de cableado ofrecerá asistencia constante al cliente cuando surgieran problemas con el cableado.

## Cableado de Enlace Permanente y Enlace de Canal

Si trabajamos con las normas que determinan el cableado estructurado, veremos que se especifican ocasionalmente diferentes restricciones o recomendaciones para el cableado de enlace permanente con respecto al enlace de canal, vemos por ejemplo que en la etapa de mapa del cableado, donde se establecen parámetros para las distancias del cableado estructurado, determina canales de hasta 90 metros o 100 metros para enlace permanente. ¿Qué diferencia hay entre uno y otro? Vamos a ello:

- El enlace permanente es el cableado que va desde la roseta (el “toma” o la cajilla de red RJ-45) de la estación de trabajo hasta su correspondiente puesto en el panel de parcheo del armario de telecomunicaciones.
- El canal es el cableado que va desde el equipo de la estación de trabajo, es decir, la tarjeta de red de la terminal propiamente dicha, hasta el elemento electrónico de la red. El canal incluye el enlace permanente y los latiguillos de parcheo en los dos extremos que permiten conectar un equipo de electrónica de red como por ejemplo un Switch con un equipo informático. El canal no incluye los equipos ni sus modulares RJ-45 hembra.

En la imagen podemos visualizar en forma más clara este esquema:

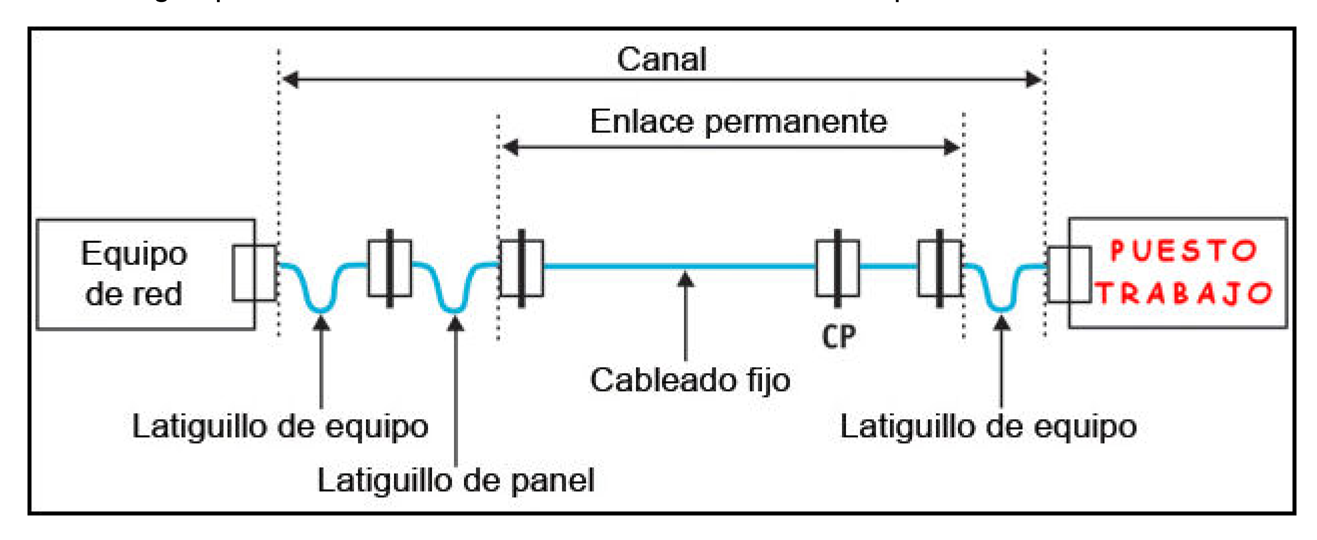



*Imagen obtenida del blog de* *[Gonzalo Nazareno]*

## Armado del cableado estructurado

A continuación, vamos a trabajar con el proceso de instalación necesario para instalar los componentes básicos de un proyecto de cableado estructurado, esta tarea comprende el armado de los cables y su posterior instalación en las correspondientes fichas y canaletas para su pasaje dentro del edificio. Trabajaremos con el armado de cables UTP como caso de estudio, el proceso para armar por ejemplo un cable de fibra óptica requiere de otros cables y otras herramientas.

Las recomendaciones para armar el cableado UTP están reguladas por la normativa EIA/TIA-568, ya que el cable en sí está compuesto por cables internos trenzados de a pares (por eso se le llama par trenzado) identificados con diferentes colores. Si no respetamos el estándar y colocamos los cables internos en cualquier orden aleatorio, pero colocamos ambos extremos del cable con el mismo orden de cables interiores, lograremos construir un cable directo funcional, pero, armar una red con cualquier otro orden que no respete la norma puede tornar complicada la comprensión de la misma para brindar mantenimiento (por ejemplo, si se rompe una ficha RJ45 y hay que cortar una parte del cable para conectar una nueva) y ni hablar si deseamos crear cables cruzados. Por lo tanto, vamos a la obra respetando la norma como debe hacerse.

La única aclaración previa, es que el orden de los colores de los cables interiores puede ser respetando el estándar EIA/TIA-568-A o bien el EIA/TIA-568B. Debemos optar por uno de ellos y armar ambos extremos del cable con el mismo orden para crear un cable directo, y con un estándar diferente en cada extremo para crear un cable cruzado.

### Cable Directo

Es la configuración que optamos para armar un cable que deseamos utilizar para conectar nuestro equipo a un switch, a un módem o a un router. También si queremos

conectar nuestra impresora a la red, o un switch a un router. Es decir, **para conectar equipos de red de diferente tipo,** usamos el cableado directo, es el más común en las redes.

## Cable Cruzado

Es el que utilizamos si queremos establecer una pequeña red entre dos computadoras, o si queremos configurar dos dispositivos que tienen la misma configuración. Típicamente se utiliza para conectar dos terminales pero también podría ocurrir que quisiéramos crear una red entre dos routers que soporten esta interfaz (Aunque generalmente entre routers se utiliza otro tipo de cable, y lo veremos más adelante). A continuación pasaremos a ver cuáles son los cables interiores que se encargan de transmitir o recibir datos, y notaremos que si armamos un cable cruzado, los cables emisores de un lado se conectan a los receptores del otro extremo y viceversa.

## Procedimiento

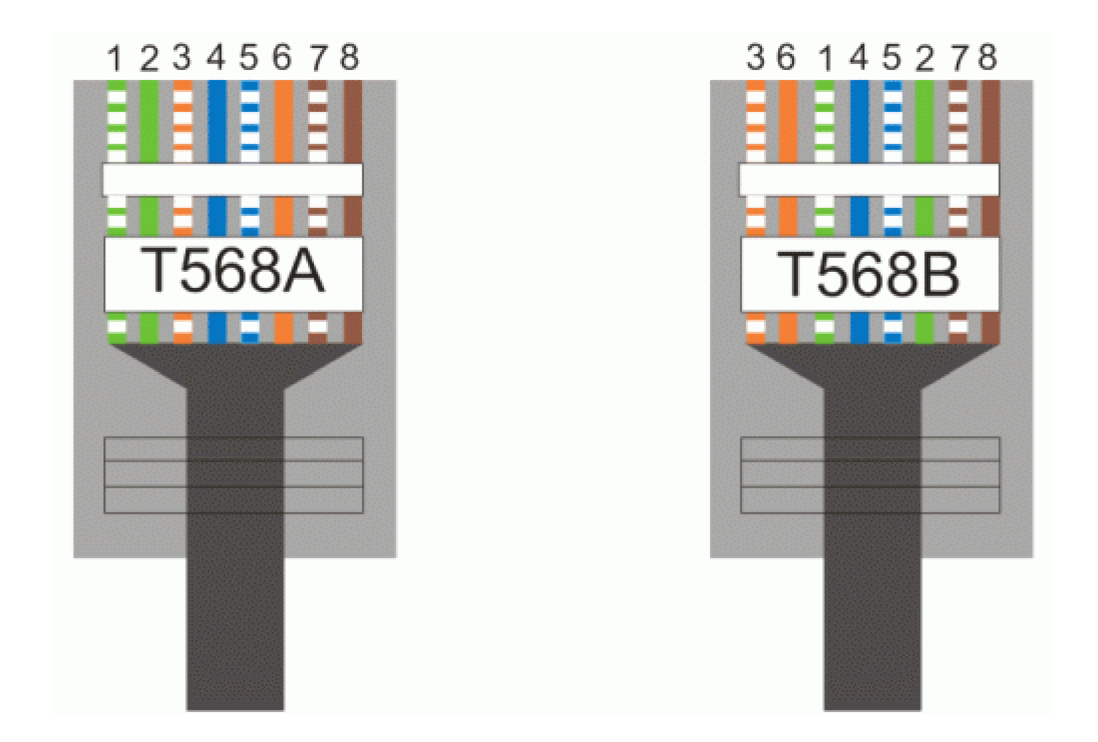
**Materiales necesarios:**

Antes de armar el cable, debemos considerar que necesitamos al menos:

- Cable UTP de la categoría deseada (recomendado 5e en adelante) la cantidad de metros deseada.
- 2 fichas de conexión RJ45
- Protectores para las fichas (simplemente a efectos de que estén recubiertas, no es imprescindible).
- Crimpadora (Pinza para armar cables de red)
- Tester de Red (no imprescindible, pero recomendado para probar el cable luego de hecho).

**Norma a elegir:**

Para armar el cable debemos considerar como antes se mencionaba, qué estándar seguir para su armado. Si colocamos sus cables interiores dentro de la ficha RJ45, y miramos la misma desde abajo, es decir, desde donde los cables van a hacer contacto con la tarjeta de red, podremos ver a través de la ficha, y para ordenar los cables en forma correcta deberemos seguir alguna de estas normas:




Como se mencionó también antes, si queremos un cable directo debemos armar ambos extremos iguales, para un cable cruzado debe haber un extremo armado según la T568A, y el otro según la T568B, los cables emisor (Tx) y receptor (Rx) podemos identificarlos en el siguiente esquema, usamos el símbolo (+) para carga positiva y (-) para carga negativa, **teniendo en cuenta el orden de los pines del estándar T568A, y considerando la numeración de la imagen anterior**:

Pin 1: TX+

Pin 2: TX-

Pin 3: RX+

Pin 4

Pin 5

Pin 6: RX-

Pin 7

Pin 8

**Procedimiento:**

- El primer paso consiste en realizar un pequeño corte sobre la goma protectora del cable UTP usando las navajas de la crimpadora, lo ideal es presionar con ésta y mover el cable en círculos para así cortarla dejando libres los pares interiores, con sumo cuidado de no cortarlos. Es decir, debemos pelar el cable UTP dejando un espacio de unos 2cm de cable interior libre.
- Si vamos a usar la funda protectora de la ficha RJ-45, debemos colocarla dentro del cable para luego cubrir la ficha.

- Debemos separar cada par trenzado cuidadosamente y estirarlos bien, colocarlos en el orden que hayamos elegido (según la norma) para colocar dentro de la ficha, y asegurarnos de que estén todos al mismo nivel (no debemos dejar que queden cables más largos que otros). Para ello los apilamos del modo que vayamos a necesitarlos y efectuamos un corte con la navaja de la pinza crimpadora.
- Cuidadosamente, introducimos los cables internos dentro de la ficha RJ-45, si queda parte de la goma protectora del cable UTP dentro de la ficha, no debemos hacernos problema (el problema sería que al contrario, hubiésemos pelado demasiado la goma y queden los cables interiores desprotegidos y vulnerables a quebraduras).
- Miramos la ficha resultante con cuidado desde abajo (el lado opuesto al clip) y nos aseguramos de que los cables hayan quedado en el orden correcto, en caso de que no, debemos retirar el cable y volver a organizar los pares.
- Si están en el orden correcto, colocamos la ficha dentro del espacio de la crimpadora destinado a ella (es probable que la crimpadora tenga espacio para armar otros tipos de cables de línea telefónica con otros estándares) y presionamos fuertemente, de modo que las pequeñas cuchillas de la ficha atraviesen las puntas de cada cable entrando en contacto con cada uno de los alambres.
- Si hemos terminado, repetimos todo el proceso anterior con el otro extremo del cable UTP, usando otra ficha.

Importante: Cuando hablamos de "cuchillas" de la ficha RJ-45, se hace referencia a las plaquetas metálicas pequeñas que se encuentran debajo de ésta, las que entran en contacto con los cables y el conector de red del equipo. En la imagen puede verse las fichas, y claramente se logran apreciar las cuchillas:



## Uso del Tester de Red

Una vez que hemos terminado ambos extremos podemos testear el cable, existen como se ha trabajado anteriormente, varios tipos posibles de pruebas a realizar sobre él.

Los analizadores más completos sirven para realizar pruebas de atenuación y distancia sobre el cable. Para ver cómo realizar este tipo de pruebas usando un tester o analizador de cables de red, se recomienda visitar el capítulo anterior sobre “Finalización – Prueba de Cable y Certificación”.

Sin embargo, existen analizadores de red más económicos y comunes, que sirven para testear que exista comunicación entre ambos extremos del cable, donde únicamente basta con encender el tester, conectar en el mismo uno de los extremos del cable, luego el otro extremo lo conectamos al conector correspondiente en la otra área del tester (lo que correspondería a la unidad remota en un DTX-1800) y observaremos que los LEDs del tester deberán encenderse una por una. En total, son 8 leds (como 8 pines tiene el cable) y si el LED se encendió en verde para cada uno de ellos, entonces el cable estaría funcionando, en caso de que no sea así, y nos indique en color anaranjado alguno de los LEDs, quiere decir que el pin correspondiente está cortado o que no quedó en contacto con las cuchillas de la ficha en alguno de los extremos (no lo crimpamos de forma correcta) por lo cual, en este último caso, será necesario observar bien cada extremo, y si encontramos que algún cable interior no está en contacto con su respectiva cuchilla, repetir el apretado (crimpado) de la ficha y en caso de que el problema persista, rearmar el cable.

## Conexión entre equipos

Una vez que tenemos el cableado preparado, estaremos listos para instalar una red doméstica. Mínimamente, una red puede estar comprendida por dos computadoras conectadas entre sí a través de un cable cruzado. Por otra parte, podemos conectar varios equipos en una red pequeña conectando cada equipo a un switch (usando cables directos al switch) y configurando los equipos.

Para que los equipos puedan encontrarse en la red, deberían estar configurados con direcciones de red lógicas (IP) capaces de verse, más adelante cuando trabajemos capa de red, trabajaremos en profundidad este protocolo. No obstante por ahora basta convenir que debemos colocar para todos una misma máscara de subred, la cual determinará cuáles son los rangos de IPs que pueden estar contenidos dentro de la misma subred. Típicamente, la máscara de subred que usaremos será la 255.255.255.0, la cual permite que en la misma subred se usen IPs que varíen en su última cifra, por ejemplo, los equipos con las direcciones 192.168.1.2 y 192.168.1.3 con esa máscara, podrán encontrarse entre sí.

Si para este caso, en lugar de un switch, usáramos un router, no sería necesario configurar las IPs en los equipos, sino que dejamos esta configuración para que la IP se obtenga automáticamente. Será el router, el dispositivo que se encargará de asignar a cada equipo una IP de manera dinámica a través de un sistema basado en un protocolo denominado DHCP, más adelante, desarrollaremos más sobre este tema.

## Crear una pequeña red local entre dos o varios equipos

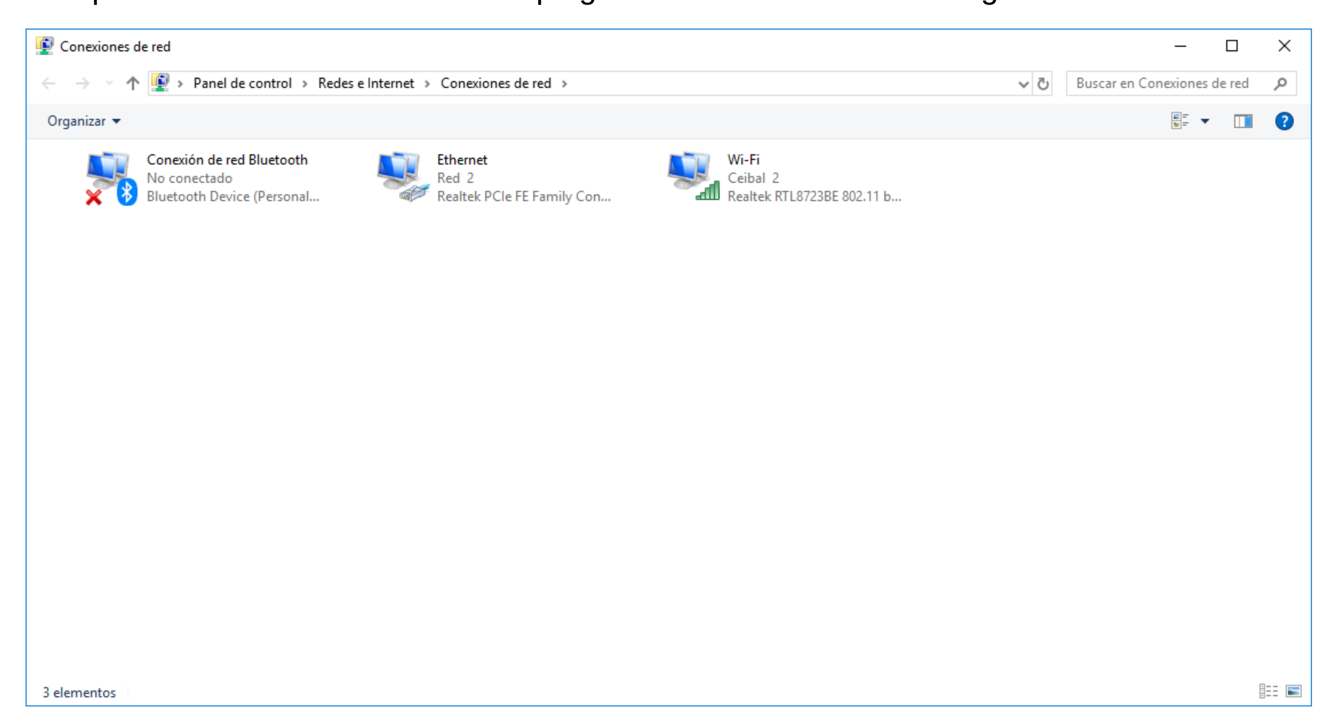
Dicho lo anterior, podemos comenzar a crear nuestra pequeña red local dependiendo de si queremos conectar dos equipos entre sí, o si queremos conectar varias computadoras en una misma red local:

### *Creando una red de dos computadoras mediante cable cruzado*

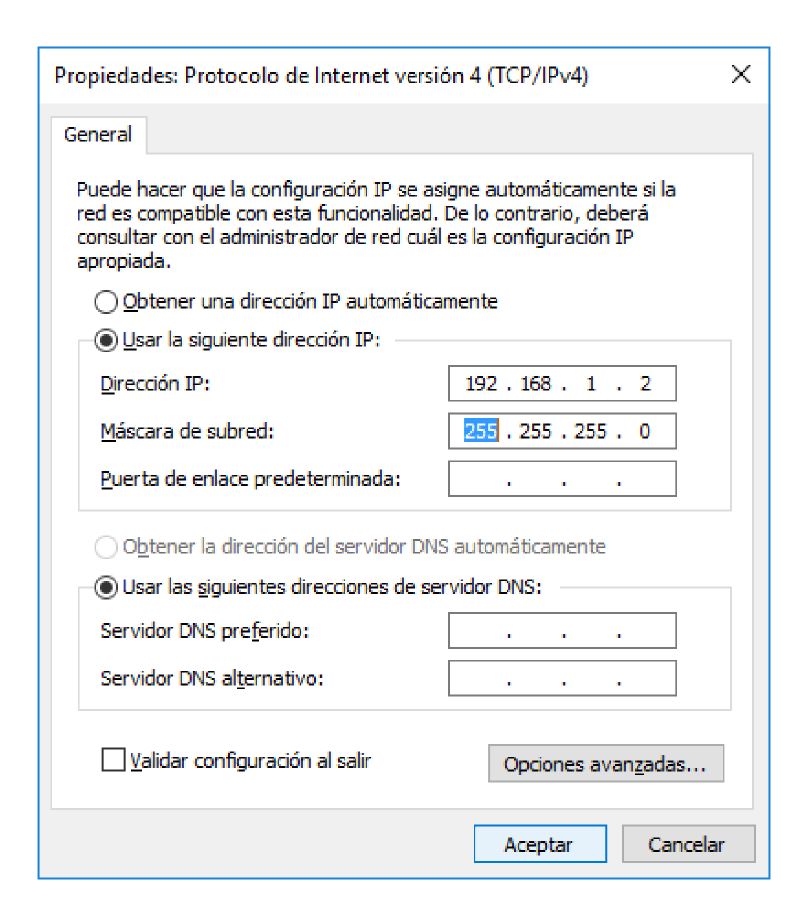
#### Configuración de las IP

Antes de conectar físicamente los equipos, debemos configurar los equipos como dijimos antes, con las IPs visibles entre sí. La configuración de las interfaces de red (tarjetas de red) de cada equipo con una respectiva IP, varía dependiendo del sistema operativo a elegir.

En Windows, debemos irnos al “Panel de Control”, luego en “Red” y a “Cambiar la Configuración del Adaptador”, entonces Windows nos desplegará la lista de las tarjetas de red que tenemos instaladas. Se desplegará una ventana como la siguiente:




Hacemos clic derecho sobre cualquiera de las tarjetas de red y a “Propiedades”. En la ventana emergente podemos seleccionar “Protocolo de Internet Versión 4 (ipv4)” y cliqueamos en el botón “Propiedades”. El programa nos mostrará entonces una ventana emergente desde la que podemos modificar nuestra IP, deberíamos hacer el mismo procedimiento en todos los equipos a conectar:




### Conectando físicamente los equipos

En el paso anterior, debemos haber configurado los equipos con IPs que se encuentren dentro de la misma subred, luego de esto, si tenemos dos equipos, simplemente conectamos un extremo del cable cruzado en cada uno de los equipos.

### Probando la velocidad de conexión con el comando PING

Posteriormente de haber configurado los equipos, pasaremos a probar la velocidad de conexión (medida en milisegundos) entre los equipos. Para ello, enviamos paquetes a otro equipo teniendo en cuenta su IP mediante el comando **ping,** para ello abrimos una terminal en Linux o la Consola de Comandos (CMD) en Windows, y tipeamos el comando con la dirección IP del equipo que queremos saber si tenemos conexión, y la velocidad, el comando sería por ejemplo:

*ping 192.168.1.3*

El comando anterior, lo podríamos utilizar por ejemplo desde el equipo con la dirección 192.168.1.2 hacia otro con la dirección 192.168.1.3. Si el tiempo de espera se agota para la solicitud que realizamos, es porque no hay conexión. Si se pierden algunos de los paquetes enviados por el programa, hay problemas de conexión, y si todos los paquetes son recibidos por el equipo de destino, entonces tenemos una conexión correcta al equipo.

## Creando una red de dos o más computadoras utilizando un switch

Podemos utilizar un switch para crear una red pequeña ya sea con dos equipos, o con más de dos, la diferencia con el método del cable cruzado es obvia, utilizar un switch

es mucho más óptimo ya que podemos conectar más de dos equipos, pero además podemos compartir Internet entre los equipos sin la necesidad de tener dos tarjetas de red en uno de los equipos (si tenemos dos equipos conectados por cable cruzado, para compartir Internet deberíamos tener instalada una segunda tarjeta de red en uno de los equipos, y a ella conectar el cable que procede de nuestro módem ADSL).

Cuando usamos un switch, el procedimiento para configurar la red a nivel del sistema operativo, será el mismo que con el cable cruzado, la diferencia radica básicamente a nivel físico, donde cada equipo, impresora, o dispositivo que se quiera conectar a la red, debe tener un cable directo conectado a una de las interfaces del switch.

En una etapa posterior de la guía, trabajaremos cómo compartir archivos y recursos a través de la red, como por ejemplo, impresoras u otros dispositivos.

## Capa de Enlace

Anteriormente se estuvo hablando sobre conexiones, cableado y estructuras para la instalación de una red. Toda la instalación física y su configuración a nivel físico hace referencia al control de acceso al medio. **La capa física,** es precisamente la que se encarga de dicho control, del flujo de bits entre dispositivos y su conexión entre sí. Ahora vamos a trabajar con la capa siguiente en el modelo de referencia OSI: La capa de Enlace de datos.

La capa de enlace es la encargada de realizar el direccionamiento físico entre los equipos, a groso modo, es la que se encarga de establecer localización entre los diferentes dispositivos de una red. ¿Cómo hace un equipo para detectar a otro dentro de una red? Cada equipo tiene su dirección, las ya mencionadas direcciones IP pueden ser dinámicas dependiendo del caso, y pueden repetirse en diferentes subredes, no obstante, las direcciones de Hardware (MAC) de cada equipo sí se trata de una dirección única, y el protocolo MAC es el correspondiente al direccionamiento que ofrece esta capa.

La capa de Enlace no sólo se encarga del direccionamiento, sino también del control de errores y de coordinar el flujo de tramas de bytes entre equipos interconectados para permitir que exista efectivamente comunicación. Así lo define Tanembaum (2014) a la función de esta capa:

*La principal tarea de la **capa de enlace** de datos es transformar un medio de transmisión puro en una línea que esté libre de errores de transmisión. Enmascara los errores reales, de manera que la capa de red no los vea. Para lograr esta tarea, el emisor divide los datos de entrada en **tramas de datos** (por lo general, de algunos cientos o miles de bytes) y transmite las tramas en forma secuencial. Si el servicio es confiable, para confirmar la recepción correcta de cada trama, el receptor devuelve una **trama de confirmación de recepción.** Otra cuestión que surge en la capa de enlace de datos (y en la mayoría de las capas superiores) es cómo evitar que un transmisor rápido inunde de*

*datos a un receptor lento. Tal vez sea necesario algún mecanismo de regulación de tráfico para notificar al transmisor cuando el receptor puede aceptar más datos.* [(Wikipedia)]

Podemos decir que los protocolos de la capa de enlace están enfocados principalmente a evitar errores en los datos enviados por un equipo, organizando el flujo de bits que se envían en bloques llamados tramas de datos, y asegurándose de que el equipo receptor reciba esas tramas de manera ordenada, encargándose de reordenar los datos en caso de colisiones o pérdida de datos en el camino.

Funciones de la capa de enlace:

Resumiendo lo anteriormente dicho, podemos aclarar que las funciones de esta capa son:

1. Proporcionar a la capa de red una interfaz de servicio bien definida.

2. Manejar los errores de transmisión.

3. Regular el flujo de datos para que los emisores rápidos no saturen a los receptores lentos.

## Ethernet como tecnología de LAN

En la mayoría de los casos, cuando hablamos de redes de manera coloquial, nos referimos a redes de área local (LAN), sin embargo, cabe aclarar que las redes de Área Local también se encuentran estandarizadas bajo un conjunto de normas que determinan las particularidades físicas y electrónicas que debe poseer una red de este tipo.

Ethernet, es precisamente el estándar que define las características de las redes locales para computadoras con control de acceso al medio por escucha de onda portadora y con detección de colisiones (CSMA/CD). Su nombre proviene del concepto físico de “ether”, que se utilizaba para referirse a una supuesta sustancia extremadamente ligera que según la física tradicional debería ocupar todo el espacio aparentemente vacío en el universo (actualmente los físicos emplean más el concepto de vacío sin tratarlo como una sustancia, por ser el medio en el que se propaga la luz a una velocidad inalcanzable para partículas con masa mayor a cero).

### CSMA/CD

Del Inglés “Carrier Sense Multiple Access With  Collision Detection” (Acceso Múltiple con escucha de portadora y detector de colisiones) es un algoritmo de acceso al medio compartido. Se utiliza en redes Ethernet para mejorar sus prestaciones y evitar colisiones de datos entre los equipos. Mediante este algoritmo, los dispositivos de red escuchan el medio antes de efectuar una transmisión, es decir,  es necesario determinar si el canal y sus recursos están disponibles antes de comenzar a transmitir.

Tipos de CSMA/CD

- ***CSMA 1-persistente****: cuando una estación quiere transmitir, primero escucha el canal. Si éste está libre entonces transmite inmediatamente. En el caso contrario permanece a la escucha hasta que esté libre. En el momento en el que la estación*

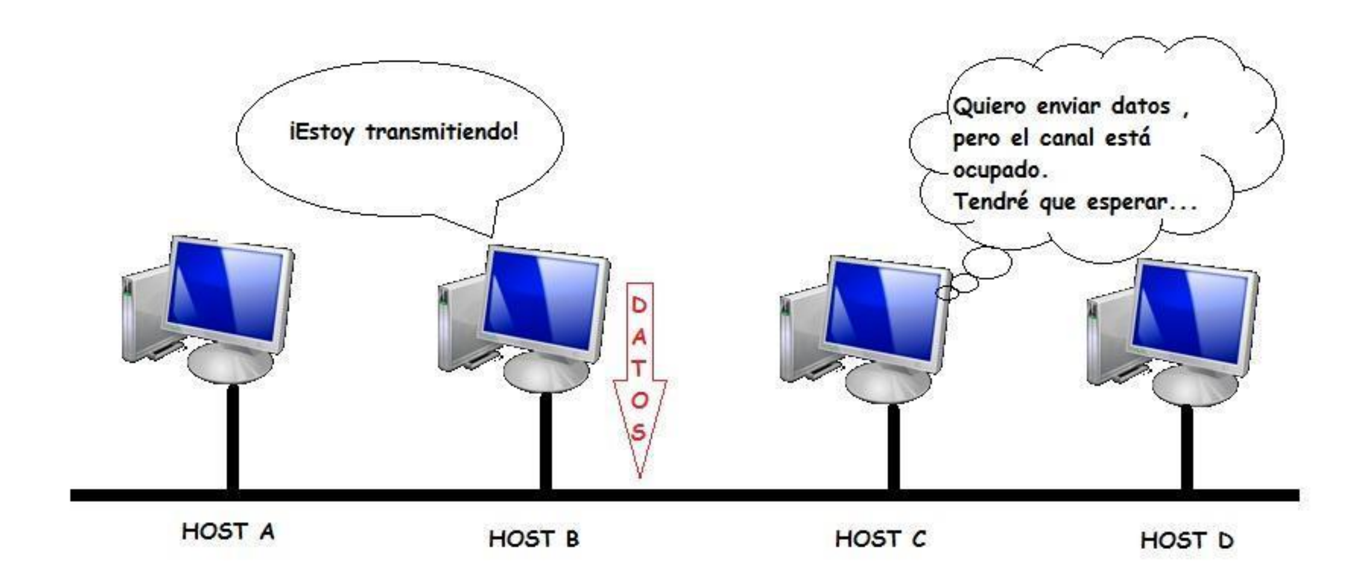
*considere que el canal está disponible, se transmite inmediatamente. El problema radica en que varias estaciones pueden estar esperando a que el canal esté libre para transmitir, dando lugar a una colisión de sus tramas.*

- ***CSMA no persistente**: funciona de forma análoga al anterior excepto en el hecho de que cuando detecta que el canal está ocupado, en vez de permanecer a la espera escuchándolo, espera un tiempo aleatorio y vuelve a escuchar el canal. Con este método se reducen las colisiones si el tráfico es elevado, mejorándose la utilización del canal. Sin embargo aumentan los retardos para cargas de tráfico bajas .*

- ***CSMA p-persistente**: al igual que en los casos anteriores se escucha el canal, sin embargo si éste está libre, en vez de transmitir inmediatamente, se transmite con una probabilidad p, o bien se retrasa la emisión una ranura temporal con una probabilidad q=1-p . Esta ranura temporal suele ser igual al máximo retardo de propagación de la señal.*

*Habitualmente suele ser utilizado el algoritmo 1-persistente, pues es empleado en el estándar .*

El siguiente ejemplo ilustra el funcionamiento del algoritmo:




<u>Conformación de las tramas CSMA/CD</u>

*La trama empleada en CSMA/CD está formada por ocho campos:*

- *El **preámbulo**, formado por 7 octetos, es el encargado de que el receptor pueda sincronizarse con el emisor, de forma que pueda localizarse el principio de la trama.*

- ***Delimitador de inicio**: es un byte empleado para indicar al receptor el inicio de la trama.*

- ***Dirección de destino**: contiene la dirección física (MAC) del equipo destinatario de la trama.*

- ***Dirección de origen****: contiene la dirección MAC de la estación emisora de la trama y tiene un formato similar al de la dirección de destino.*

- ***Longitud****: indica la longitud del campo de datos que se encuentra a continuación. Es necesaria para determinar la longitud del campo de datos en los casos que se utiliza un campo de relleno.*

- ***Información****: contiene los datos transmitidos. Es de longitud variable, por lo que puede tener cualquier longitud entre 42 y 1500 bytes.*

- ***Relleno****: es usado para que la trama alcance la longitud mínima requerida. Una trama debe contener un mínimo número de bytes para que las estaciones puedan detectar las colisiones con precisión.*

- ***Chequeo****: contiene un código de redundancia cíclica de 32 bits. Es utilizada como mecanismo de control de errores en la transmisión*

*Imágenes e Información obtenidas de* Wikipedia

## Estándar IEEE 802.3

La IEEE "Institute Of Electricals and Electronic Engineers" o el Instituto de Ingenieros Eléctricos y Electrónicos diseñaron desde 1983 el IEEE 802.3, un estándar de comunicaciones para redes basadas en Ethernet, el cual fue cambiándose y actualizándose con el paso del tiempo para cubrir las nuevas tecnologías que implicaban cambios en las velocidades de transmisión y dispositivos de conexión de redes y enrutamiento, redes virtuales, además de cambios en los medios físicos (pasaje de soporte de cables de cobre en sus diferentes calidades y luego de fibra óptica).

Lista de cambios conocidos hasta el momento:

| Estándar Ethernet | Fecha | Descripción |
|---|---|---|
| Ethernet experimental | 1972 (patentado en 1978) | 2,85 Mbit/s sobre cable coaxial en topología de bus. |
| Ethernet II (DIX v2.0) | 1982 | 10 Mbit/s sobre coaxial fino (thinnet) - La trama tiene un campo de tipo de paquete. El protocolo IP usa este formato de trama sobre cualquier medio. |

| | | |
|---|---|---|
| IEEE 802.3 | 1983 | 10BASE5 10 Mbit/s sobre coaxial grueso (thicknet). Longitud máxima del segmento 500 metros - Igual que DIX salvo que el campo de Tipo se substituye por la longitud. |
| 802.3a | 1985 | 10BASE2 10 Mbit/s sobre coaxial fino (thinnet o cheapernet). Longitud máxima del segmento 185 metros |
| 802.3b | 1985 | 10BROAD36 |
| 802.3c | 1985 | Especificación de repetidores de 10 Mbit/s |
| 802.3d | 1987 | FOIRL (*Fiber-Optic Inter-Repeater Link*) enlace de fibra óptica entre repetidores. |
| 802.3e | 1987 | 1BASE5 o StarLAN |
| 802.3i | 1990 | 10BASE-T 10 Mbit/s sobre par trenzado no blindado (*Unshielded Twisted Pair* o UTP). Longitud máxima del segmento 150 metros. |
| 802.3j | 1993 | 10BASE-F 10 Mbit/s sobre fibra óptica. Longitud máxima del segmento 1000 metros. |
| 802.3u | 1995 | 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s con auto-negociación de velocidad. |
| 802.3x | 1997 | Full Duplex (Transmisión y recepción simultáneos) y control de flujo. |
| 802.3y | 1998 | 100BASE-T2 100 Mbit/s sobre par trenzado no blindado (UTP). Longitud máxima del segmento 100 metros |
| 802.3z | 1998 | 1000BASE-X Ethernet de 1 Gbit/s sobre fibra óptica. |
| 802.3ab | 1999 | 1000BASE-T Ethernet de 1 Gbit/s sobre par trenzado no blindado |

| | | |
|---|---|---|
| 802.3ac | 1999 | Extensión de la trama máxima a 1522 bytes (para permitir las "Q-tag") Las Q-tag incluyen información para 802.1Q VLAN y manejan prioridades según el estándar 802.1p. |
| 802.3ad | 2000 | Agregación de enlaces paralelos. |
| 802.3ae | 2003 | Ethernet a 10 Gbit/s ; 10GBASE-SR, 10GBASE-LR |
| IEEE 802.3af | 2003 | Alimentación sobre Ethernet (PoE). |
| 802.3ah | 2004 | Ethernet en la última milla. |
| 802.3ak | 2004 | 10GBASE-CX4 Ethernet a 10 Gbit/s sobre cable bi-axial. |
| 802.3an | 2006 | 10GBASE-T Ethernet a 10 Gbit/s sobre par trenzado no blindado (UTP) |
| 802.3ap | en proceso (draft) | Ethernet de 1 y 10 Gbit/s sobre circuito impreso. |
| 802.3aq | en proceso (draft) | 10GBASE-LRM Ethernet a 10 Gbit/s sobre fibra óptica multimodo. |
| 802.3ar | en proceso (draft) | Gestión de Congestión |
| 802.3as | en proceso (draft) | Extensión de la trama |

*Tabla Obtenida de WIkipedia*

## Tramas en Ethernet y en 802.3

Las diferencias entre los estilos de tramas de Ethernet original y el IEEE 802.3 revisado son mínimas, esta diferencia es lo suficientemente significativa como para hacer a las dos versiones incompatibles. La diferencia más significativa entre Ethernet original y el IEEE 802.3 revisado es el agregado de un delimitador de inicio de trama (SFD) y un pequeño cambio en el campo Tipo que incluye la Longitud.

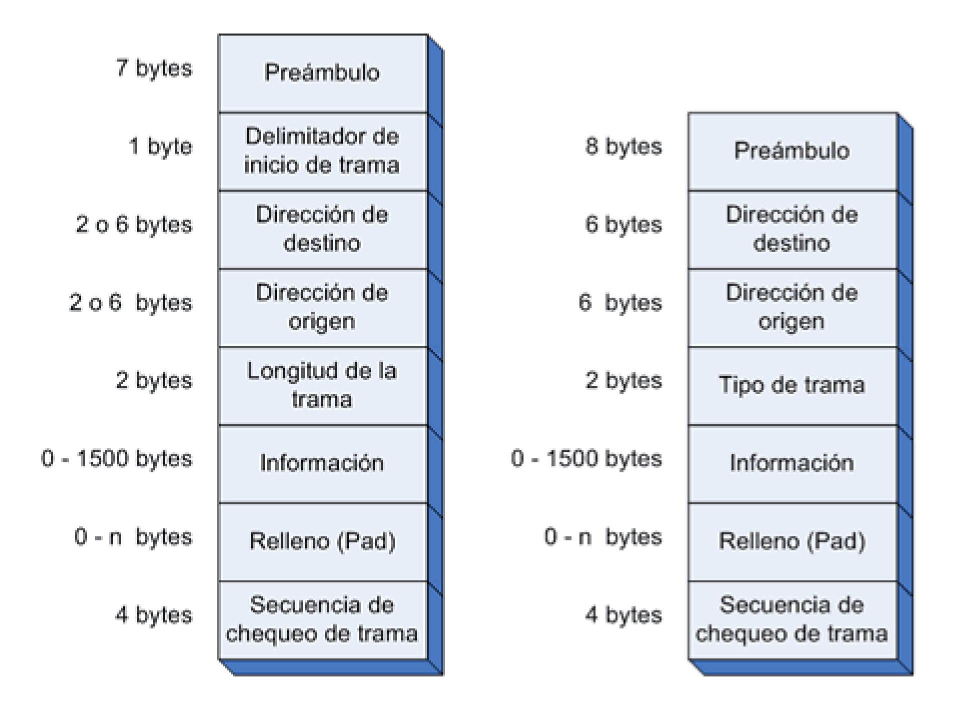



*Imagen obtenida del blog* TechClub

## Colisiones y Dominio de Colisiones

Las colisiones en una red son también conocidas como la “interferencia”, típicamente ocurren cuando dos equipos logran enviar una trama de manera simultánea. La palabra “Colisión” de hecho ya nos trae a la mente la idea de un choque, de ocurrencia simultánea de dos o más objetos en un mismo y momento y lugar donde no deberían ocurrir. Obviamente existen dispositivos que permiten evitar las colisiones y algoritmos que las reducen, los cuales se fueron mejorando y extendiendo a medida que avanzan las tecnologías de telecomunicaciones.

“*Un **dominio de colisión** es un segmento físico de una red de computadores donde es posible que las tramas puedan "colisionar" (interferir) con otros. Estas colisiones se dan particularmente en el protocolo de red Ethernet.*

*A medida que aumenta el número de nodos que pueden transmitir en un segmento de red, aumentan las posibilidades de que dos de ellos transmitan a la vez. Esta transmisión simultánea ocasiona una interferencia entre las señales de ambos nodos, que se conoce como colisión. Conforme aumenta el número de colisiones disminuye el rendimiento de la red.*

*El rendimiento de una red puede ser expresado como :*

***Rendimiento (%) = [1 - (Colisiones / Paquetes Totales) ] * 100***

*Un dominio de colisión puede estar constituido por un solo segmento de cable Ethernet en una Ethernet de medio compartido, o todos los nodos que afluyen a un concentrador*

*Ethernet en una Ethernet de par trenzado, o incluso todos los nodos que afluyen a una red de concentradores y repetidores.”*

*Información sobre Dominio de Colisiones extraída de* Wikipedia

## Funcionamiento de un HUB

El hub es también conocido en habla hispana como **concentrador**, ya que es un dispositivo de red que se encarga precisamente de eso, de servir como punto de concentración de todos los cables provenientes de las terminales de una red local. Únicamente se encarga de realizar conexión física, sin mayor complejidad, recibe una señal por una de sus entradas y la retransmite a todas las demás. En la actualidad, para la mayoría de los usos, se han sustituido por los switches (conmutadores) que poseen funcionalidades más complejas.

El concentrador es un dispositivo de capa 1, capa física en el modelo OSI, o capa de acceso al medio en el modelo de referencia TCP/IP, ya que únicamente se encarga de realizar conexión física y de retransmitir señales, no obstante, no realiza direccionamiento ni ruteo.

Frente a otros dispositivos similares de capas superiores, tiene la desventaja de que una misma señal la retransmite a todos los equipos y no sólo al equipo de destino, incurriendo aquí en un problema de seguridad, por otro lado, es mucho más susceptible a colisiones de datos, y no es capaz de corregir errores producidos por éstas.

### Usos en la actualidad

Si bien el uso de hubs para redes de oficina pequeñas ha sido sustituído por los conmutadores, por su eficiencia, actualmente existen fines para los cuales es más aconsejable utilizar un hub, por ser mucho más barato o simplemente por que increíblemente, facilitan más la tarea, estos casos particulares son:

- *Un analizador de protocolo conectado a un conmutador no siempre recibe todos los paquetes, ya que desde que el conmutador separa a los puertos en los diferentes segmentos. En cambio, la conexión del analizador de protocolos con un concentrador permite ver todo el tráfico en el segmento. Por otra parte, los conmutadores caros pueden ser configurados para permitir a un puerto escuchar el tráfico de otro puerto (lo que se denomina puerto de duplicado); sin embargo, esto supone un gasto mucho más elevado que si se emplean concentradores.*
- *Algunos grupos de computadoras o clúster, requieren cada uno de los miembros del equipo para recibir todo el tráfico que trata de ir a la agrupación. Un concentrador hará esto, naturalmente; usar un conmutador en estos casos, requiere la aplicación de trucos especiales.*
- *Cuando un conmutador es accesible para los usuarios finales para hacer las conexiones, por ejemplo, en una sala de conferencias, un usuario inexperto puede reducir la red mediante la conexión de dos puertos juntos, provocando un bucle. Esto puede evitarse usando un concentrador, donde un bucle se romperá en el concentrador para los otros usuarios (también puede ser impedida por la*

*compra de conmutadores que pueden detectar y hacer frente a los bucles, por ejemplo mediante la aplicación de Spanning Tree Protocol).*

*Información extraída de* Wikipedia

Estéticamente, un hub es casi idéntico al de un switch, ya que a la vista son simplemente dispositivos con varias interfaces de red con el fin de realizar las conexiones:



*Imagen extraída de la web* PC-Code

## Funcionamiento de un SWITCH

El switch al igual que el hub permite conectar varias terminales de una red a nivel físico, pero además posee otras funcionalidades como ser el direccionamiento de las señales a este nivel, lo que optimiza la retransmisión de datos, siendo que a una señal entrante la lleva a la salida de destino, en lugar de todas las salidas.

Es un dispositivo de la capa de enlace de datos, es decir, de capa 2, ya que opera con tramas de datos, en las cuales encuentra la dirección de hardware (MAC) de destino de una trama, y a través de dicha dirección, optimiza la entrega de dicha trama. Por otro lado, libera la conexión una vez que dicha trama fue entregada, permitiendo la optimización de los recursos de red, y disminuyendo la probabilidad de la existencia de colisiones.

Además de ser popularmente usados para redes locales de una sola oficina, los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Esto ocurre al igual que los puentes, dado que funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red. Esto es especialmente útil cuando se está en un área que ocupa varias oficinas para conectar en red a todas ellas y compartir recursos. Por ejemplo, en una Escuela puede observarse generalmente que la red parte de un área principal donde se encuentra la conexión a Internet, y también un switch, y a dicho switch,

se conectan cables que luego van dirigidos a salones independientes que también cuentan con un switch, al que se conectan las terminales.

Un punto importante sobre su funcionamiento, es que que el conmutador (switch) almacena las direcciones MAC de todos los equipos conectados, incluso si se encuentra conectado a otro conmutador (o un concentrador), guardando las direcciones MAC de los dispositivos que a su vez se encuentren conectados a éstos.

<u>Bucles de red e inundaciones de tráfico</u>

Una de las pocas problemáticas que pueden ofrecer este tipo de dispositivos son los bucles, que pueden ocurrir cuando existen varios conmutadores conectados entre sí. Como carecen de mecanismos de ruteo, se pueden habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de switches. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, éste vuelve a enviar la trama por los puertos que permiten alcanzar el equipo.

Este tipo de problemas, provoca que una trama se multiplique de manera exponencial, produciendo lo que se conoce como inundación, que acaba causando fallos o incluso una total caída de las comunicaciones.

Existen sin embargo, conmutadores más avanzados y costosos que incluyen funcionalidades típicas de routers, que poseen características de capa 3 (red) del modelo OSI, éstos, poseen mecanismos de ruteo y de corrección de errores, a diferencia de los conmutadores tradicionales, que únicamente realizan direccionamiento lógico.

*Son los conmutadores que, además de las funciones tradicionales de la capa 2, incorporan algunas funciones de enrutamiento o routing, como por ejemplo la determinación del camino basado en informaciones de capa de red (capa 3 del modelo OSI), validación de la integridad del cableado de la capa 3 por checksum y soporte a los protocolos de routing tradicionales (RIP, OSPF, etc)*

*Los conmutadores de capa 3 soportan también la definición de redes virtuales (VLAN), y según modelos posibilitan la comunicación entre las diversas VLAN sin la necesidad de utilizar un router externo.*

*Por permitir la unión de segmentos de diferentes dominios de difusión o broadcast, los switches de capa 3 son particularmente recomendados para la segmentación de redes LAN muy grandes, donde la simple utilización de switches de capa 2 provocaría una pérdida de rendimiento y eficiencia de la ADSL, debido a la cantidad excesiva de broadcasts.*

*Se puede afirmar que la implementación típica de un switch de capa 3 es más escalable que un enrutador, pues este último utiliza las técnicas de enrutamiento a nivel 3 y enrutamiento a nivel 2 como complementos, mientras que los switches sobreponen la función de enrutamiento encima del encaminamiento, aplicando el primero donde sea necesario.*

*Información en cursiva extraída de* [Wikipedia]

## Modos de funcionamiento de un SWITCH

Atendiendo al método de funcionamiento de las tramas utilizadas, hay diversos tipos de conmutadores, a saber:

### *Store and Forward*

Del Inglés "Almacenamiento y reenvío", guardan cada trama en un búfer antes del intercambio de información hacia el puerto de salida. Mientras la trama está en el búfer, el switch calcula su CRC mide el tamaño de la misma. Si el CRC falla, o el tamaño es muy pequeño o muy grande (una trama Ethernet tiene entre 64 bytes y 1518 bytes) la trama es descartada. Si todo se encuentra en orden es encaminada hacia el puerto de salida.

Este método asegura operaciones sin error y aumenta la confianza de la red. Pero el tiempo utilizado para guardar y chequear cada trama añade un tiempo de demora importante al procesamiento de las mismas. La demora o delay total es proporcional al tamaño de las tramas: cuanto mayor es la trama, más tiempo toma este proceso.

### *Cut-Through*

Del Inglés "Romper", este mecanismo es más veloz que el anterior, ya que va enviando una trama antes de haberla recibido por completo, leídos los primeros 6 bytes de una trama, ya tienen conocida la dirección MAC de destino y la encaminan. El problema de este modo es que no permite calcular posibles errores en una trama causados por colisiones, ni errores de CRC, reenviando tramas con fallos a los dispositivos de destino (estas son llamadas, tramas corruptas), a más errores existan en la red, mayor ancho de banda será consumido por tramas corruptas.

Este mecanismo fue corregido por switch más avanzados de este tipo, conocidos como **fragment free**, estos últimos, leen los primeros 64 bytes de cada trama antes de ser enviada (que es el tamaño mínimo total de las tramas), de modo que puede aplicar algoritmos de detección de errores sobre ella y así evitando transmitir tramas corruptas.

### *Adaptive Cut-Through*

Estos conmutadores procesan tramas en modo adaptativo, es decir, pueden emplear cualquiera de los dos mecanismos antes desarrollados. En algunos switches, es el operador de red quién debe configurarlos para usar el método Store-And-Forward o bien por Cut-Through, y en otros casos, el conmutador es lo suficientemente "inteligente" para seleccionar el modo que sea más eficiente para la red en cuestión, esto último dependerá de la cantidad de colisiones existentes en la red. En redes con un bajo número de colisiones se utilizará el método Cut-Through por ser más rápido, pero si el número de colisiones supera una cantidad admisible el switch puede configurarse como Store-And-Forward y evitar errores de modo más inteligente.

*Importante: Los conmutadores cut-through son más utilizados en pequeños grupos de trabajo y pequeños departamentos. En esas aplicaciones es necesario un buen volumen*

*de trabajo o throughput, ya que los errores potenciales de red quedan en el nivel del segmento, sin impactar la red corporativa.*

*Los conmutadores store-and-forward son utilizados en redes corporativas, donde es necesario un control de errores.*

## Configurando un SWITCH Cisco

Para este apartado se aclarará ante todo que existen pequeños conmutadores con pocas salidas de red, de bajo costo, que son útiles para crear redes pequeñas dentro de una misma oficina pequeña; éstos no requieren de demasiada configuración, sino que simplemente se conectan los equipos al switch y debemos configurar manualmente las direcciones IP de cada equipo. Así todos podrán encontrarse bajo el mismo rango de IP, y efectivamente pueda existir comunicación entre ellos.

Para este caso de estudio, se desarrollará un ejemplo de configuración inicial para un switch de tipo CISCO, con funcionalidades de nivel 3.

**Configuración inicial del switch:**

Antes de empezar a configurar el switch debemos tener en cuenta que hay parámetros que pueden variar dependiendo de la marca y modelo del switch, por ende es importante contar con el manual del dispositivo, y en caso de no tenerlo, descargarlo de Internet (En el caso de los conmutadores CISCO, el manual de cada modelo al igual que todo el software necesario para configurar la red desde el entorno gráfico están disponibles libremente desde la *Web Oficial.*

Para nuestro caso de estudio, se utilizará un CISCO Catalyst series 2960, un modelo de conmutador de 26 interfaces que ya viene con un sistema operativo iOS previamente configurado para ser utilizado para interconectar redes. Sin embargo, el sistema permite configurar el switch de manera personalizada para obtener diferentes funcionalidades, un switch de estas características puede ser configurado tanto como DCE como DTE, se pueden cambiar los rangos de IP que manejaran las diferentes interfaces de red, incluso puede ser configurado para tener diferentes subredes operando conectadas físicamente hacia el mismo switch. Esto se logra gracias a que los dispositivos Cisco permiten separar varias redes lógicas o virtuales (VLANs) para una misma red física, creando una división real entre los equipos que físicamente están sobre una misma red.

Dicho modelo de conmutador, permite configurarse de varios modos diferentes, a saber, el switch admite dos modos de configuración fundamentales:

- El modo express setup – Que implica conectar una PC al switch a través de un cable de red y configurarlo desde la interfaz gráfica.
- El modo consola – Que implica conectar la PC al switch con un cable de serie al puerto de consola del switch (dicho cable viene provisto con el switch y tiene un extremo con conector de seire DB-9 y otro extremo RJ-45 que va al puerto del switch). Este método se detallará pues requiere del ingreso de comandos y es el

que tendremos por seguro para dar la configuración inicial a cualquier dispositivo Cisco.

## Configuración inicial por consola

A modo genérico, se desarrollará a continuación los pasos necesarios para configurar básicamente un conmutador Cisco, pero igualmente se recomienda seguir al pie de la letra las indicaciones de su manual.

Primero se debe realizar la conexión física entre el conmutador y la computadora. Necesitamos para ello una computadora que tenga puerto serial hembra (o un adaptador USB a DB-9 si la PC carece de este conector), un software de emulación de terminal (como por ejemplo HyperTerminal) y el cable que va desde el puerto de Consola del switch al puerto de serie de la PC. Este último, suele tener en un extremo un conector DB-9 para la PC y en el otro un conector RJ45 para el switch (que no se conecta en ninguno de sus salidas para terminales, sino en su salida de CONSOLA).

Una vez que conectamos el cable de consola al puerto COM1 (serial) de la computadora, debemos abrir una terminal con la siguiente configuración:

- El puerto COM adecuado
- 9600 bps de transferencia de datos
- 8 bits de datos
- Sin paridad
- 1 bit de parada
- Sin control de flujo.

## Comandos genéricos

A continuación se detallará brevemente algunos comandos generales para configurar un Switch de Cisco a nivel genérico, como se mencionaba anteriormente, para este caso de estudio se utilizará un Catalyst 2960, el cual puede configurarse totalmente por comandos como por interfaz gráfica, no obstante, su sistema permite que la configuración por consola sea tan sencilla, que ni siquiera sea necesario tomar en cuenta los comandos que aquí se detallarán, ya que al iniciarse una sesión por consola para su configuración inicial, el mismo swtich nos va guiando y solicitando la información necesaria para configurarse.

Debido a lo anterior, se tomará como ejemplo la configuración de un modelo anterior, el 2950, y se usará como base la ejemplificación desarrollada en el blog de *Arnaldo Marquez* (se recomienda visitar para obtener información más detallada).

Como nota previa, cabe señalar que los comandos se escribirán con fuente `Courier New,` por ser más familiar a las interfaces de consola y entornos de desarrollo, y en el caso de la información que el sistema nos muestra luego de ejecutar un comando, se utilizará con estilo *`cursiva`*.

1. **Configuración del usuario y contraseña:**

   La asignación de un nombre exclusivo al Switch y las contraseñas correspondientes se realiza en el modo de configuración global, mediante los siguientes comandos:
   **Nota: El comando "enable" nos hace entrar a modo privilegiado y luego nos cambia el prompt de la consola de "Switch>" por "Switch#".**

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname NOMBRE_HOST
NOMBRE_HOST(config)#enable password [nombre de la enable
pass]
NOMBRE_HOST(config)#enable secret [nombre de la enable
secret]
NOMBRE_HOST(config)#line console 0
NOMBRE_HOST(config-line)#login
NOMBRE_HOST(config-line)#password [nombre de la pass de
consola]
NOMBRE_HOST(config)#line vty 0 4
NOMBRE_HOST(config-line)#login
NOMBRE_HOST(config-line)#password [nombre de la pass de
telnet]
```

2. **Asignación de las Direcciones IP**

Las IP en los conmutadores CISCO se implementan sobre tecnologías Virtual LAN (VLAN). Una VLAN es como el nombre lo indica, redes locales virtuales. Podemos tener una VLAN para nuestra red LAN, o varias VLAN, creando redes virtuales diferentes, donde los equipos de las diferentes redes virtuales no son accesibles entre sí. Podemos decir que una VLAN es una agrupación lógica de dispositivos que se pueden comunicar en sí.

Por defecto, la vlan 1 será la vlan del switch, aunque podemos crear más vlan y configurar las interfaces de red del switch para las diferentes vlan:

En un switch 2950:

```
SW_2950(config)#interface vlan 1
SW_2950(config-vlan)#ip address [direccion ip + mascara]
SW_2950(config-vlan)#no shutdown
```

Si el switch necesita enviar información a una red diferente a la de administración se debe configurar un gateway:

```
SW_2950(config)#ip default-gateway [IP de gateway]
```

3. **Configuración de puertos:**

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#speed [10 | 100 | auto]
Switch(config-if)#duplex [full | half | auto]
```

4. **Seguridad de puertos:**

El comando switchport port-security permite asociar la primera dirección MAC a dicho puerto:

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport port-security
```

La cantidad posibles de direcciones MAC asociadas al puerto tiene un valor comprendido entre 1 y 132, el comando switchport port-security maximun permite establecer la cantidad máxima permitida.

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport port-security maximum 10
```

En el caso de que se detecte algún intento de violación del puerto se puede ejecutar el siguiente comando, haciendo que el puerto quede automáticamente cerrado:

```
Switch(config-if)#switchport port-security violation
[protect|restrict|shutdown]
```

5. **Configurando las interfaces:**

Las interfaces del dispositivo forman parte de las redes que están directamente conectadas a él.
Estas interfaces activas deben llevar una dirección IP y su correspondiente mascara, como un host perteneciente a esa red. El administrador debe habilitar administrativamente la interfaz con el comando no shutdown, si fuera necesario la interfaz podrá deshabilitarse con el comando shutdown.
A continuación vemos la configuración de una interfaz Ethernet

```
NOMBRE_HOST>enable
Password:*******
NOMBRE_HOST#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

NOMBRE_HOST(config)#interface ethernet 0
NOMBRE_HOST(config-if)#ip address 192.168.1.1 255.255.255.0
NOMBRE_HOST(config-if)#no shutdown
NOMBRE_HOST(config-if)#description
NOMBRE_HOST(config-if)#description INTERFAZ_DE_LAN
```

El comando `show interfaces ethernet 0` muestra en la primer línea como la interfaz esta UP administrativamente y UP físicamente. Recuerde que si la interfaz no estuviera conectada o si existen problemas de conectividad el segundo UP aparecería como down.

La tercera línea muestra la descripción configurada a modo de comentario puesto que solo tiene carácter informativo y NO afecta al funcionamiento del dispositivo.

Tener acceso a la información detallada puede tener cierta importancia para los administradores a la hora de solucionas problemas.

Debajo puede apreciarse la dirección IP, encapsulación, paquetes enviados, recibidos, etc.

```
show interfaces ethernet 0
     Ethernet0 is up, line protocol is up

     Hardware is Lance, address is 0000.0cfb.6c19 (bia
     0000.0cfb.6c19)
     Description: INTERFAZ_DE_LAN
     Internet address is 192.168.1.1/24
     MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 183/255,
     load 1/255
     Encapsulation ARPA, loopback not set, keepalive set (10 sec)
     ARP type: ARPA, ARP Timeout 04:00:00
     Last input never, output 00:00:03, output hang never
     Last clearing of "show interface" counters never
     Queueing strategy: fifo
     Output queue 0/40, 0 drops; input queue 0/75, 0 drops
     5 minute input rate 0 bits/sec, 0 packets/sec
     5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
0 input packets with dribble condition detected
188 packets output, 30385 bytes, 0 underruns
188 output errors, 0 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred
188 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Si el administrador deshabilita la interfaz se vería:

```
Ethernet0 is administratively down, line protocol is down
Hardware is Lance, address is 0000.0cfb.6c19 (bia
0000.0cfb.6c19)
Description: INTERFAZ_DE_LAN
Internet address is 192.168.1.1/24
. . . . . . . . . . . . . . . . .
```

Las interfaces seriales se configuran siguiendo el mismo proceso que las ethernet, se bebe tener especial cuidado para determinar quién es el DCE (equipo de comunicaciones) y quien el DTE (equipo Terminal del abonado) debido a que el DCE lleva el sincronismo de la comunicación, este se configurara solo en la interfaz serial del DCE, el comando clock rate activara el sincronismo en ese enlace.

Clock rate Vs ancho de banda: Recuerde que existe un comando bandwidth para la configuración del ancho de banda, el router solo lo utilizara para el cálculo de costes y métricas para los protocolos de enrutamiento, mientras que el clock rate brinda la verdadera velocidad del enlace.

A continuación se observa la configuración de un enlace serial como DCE:

```
NOMBRE_HOST(config)#interface serial 0
NOMBRE_HOST(config-if)#ip address 170.16.2.1 255.255.0.0
NOMBRE_HOST(config-if)#clock rate 56000
NOMBRE_HOST(config-if)#bandwidth 100000
NOMBRE_HOST(config-if)#description RED_SERVIDORES
NOMBRE_HOST(config-if)#no shutdown
```

Algunos router llevan incorporados slots o ranuras para ampliar la cantidad de puertos,
en ese caso las interfaces se identificaran con 0/0, esto hace referencia al slot 0, interfaz 0.

### *Eliminación de la configuración de la NVRAM*

Si queremos eliminar la configuración anterior debido a errores cometidos, o si simplemente estamos probando realizar cambios en la configuración y queremos borrar las operaciones registradas en la NVRAM, realizamos:

```
Switch#erase startup-config
```

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
Erase of nvram: complete
```

Otro método más nuevo de realizar lo mismo, es simplemente tipeando el comando "`erase nvram`" en lugar de "`erase startup-config`", produce el mismo resultado.

*A pesar de eliminar la configuración de la NVRAM las VLANS no se eliminan debido a que se guardan en un archivo en la memoria flash llamado VLAN.dat.*

## Configuración inicial de un Cisco Catalyst 2960

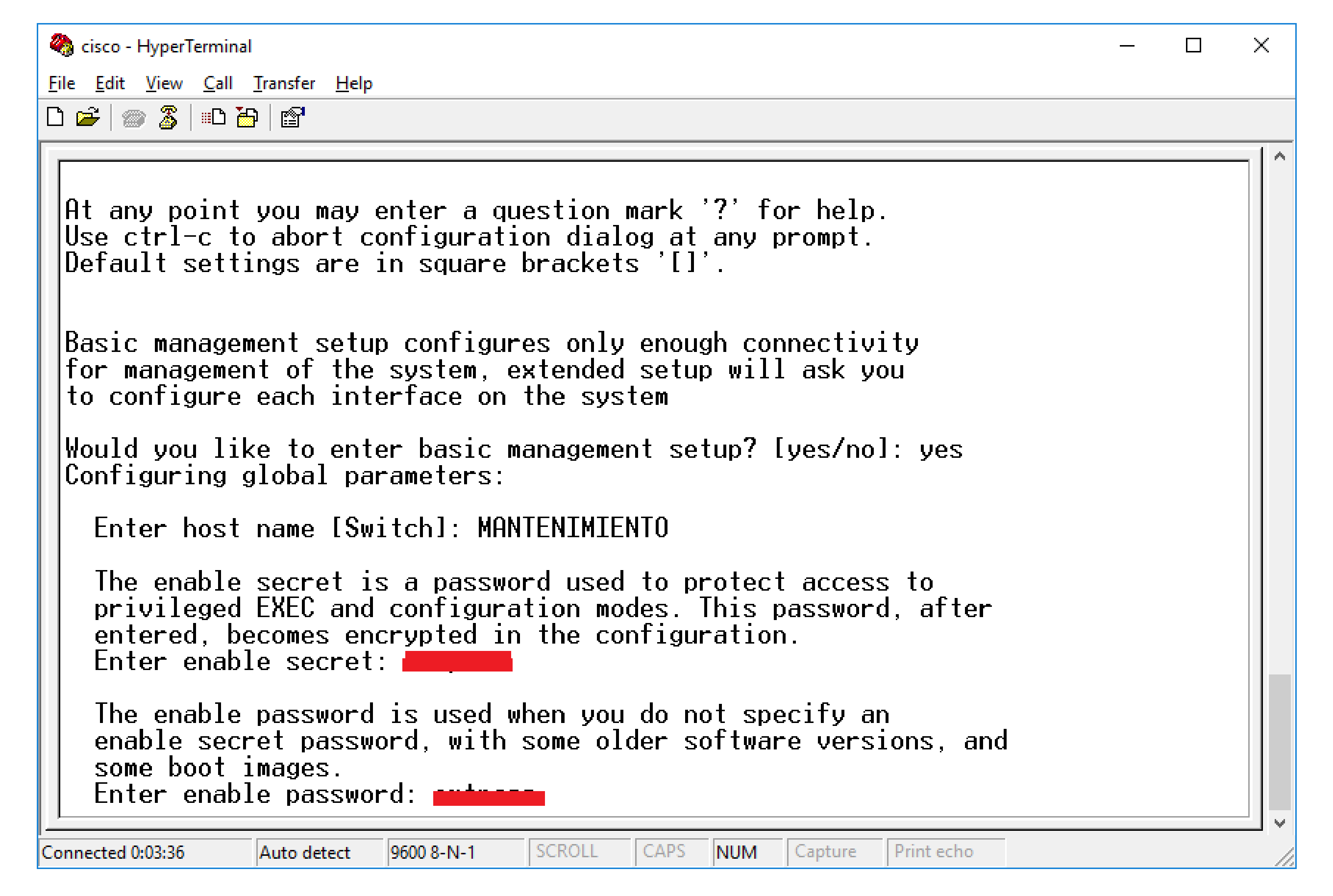
Una vez que ya se ha tratado el tema de la configuración de un Cisco desde la consola con algunos comandos genéricos, se detallará la configuración que podemos emplear para inicializar un switch 2960 para configurar una LAN de una sala de clases de Informática, para conectar varias computadoras en red, y proveerlas de Internet, en este caso particular, el switch suministrará internet proveniente de un cable desde otro switch alojado en otra parte del edificio.

Podremos ver a continuación, la configuración inicial guiada por el mismo sistema, con el cable serial conectado al PC y ninguna interfaz de red conectada.

Cabe señalar, que la configuración de la terminal es igual que para el caso anterior:

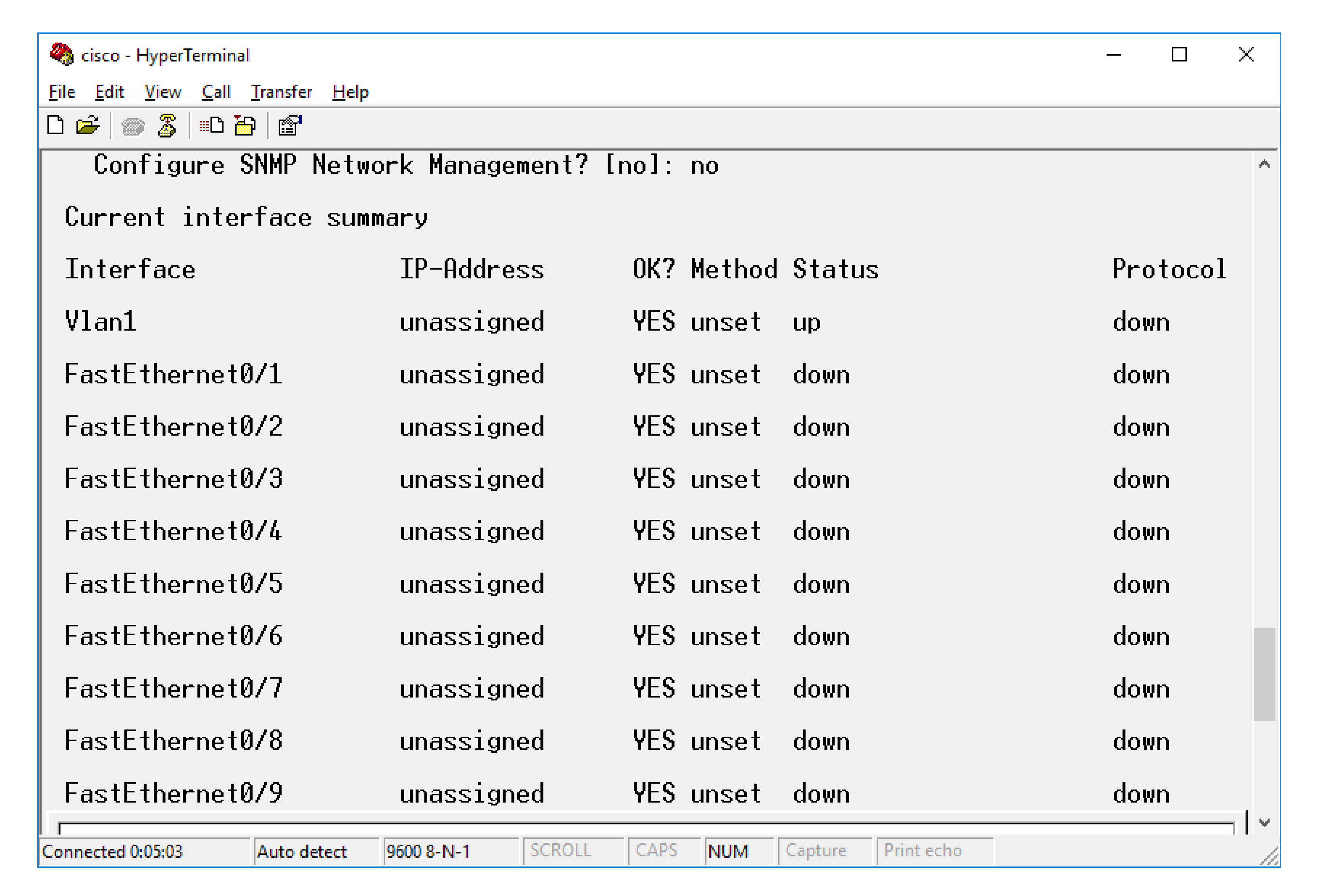
- El puerto COM adecuado (en nuestro caso COM1)
- 9600 baudios
- 8 bits de datos
- Sin paridad
- 1 bit de parada
- Sin control de flujo.

En la siguiente captura del programa HyperTerminal hemos guardado la configuración anterior bajo el nombre "cisco", vemos que lo primero que nos solicita el sistema es el ingreso del nombre del host, colocamos "MANTENIMIENTO"; ya que se va a utilizar en este ejemplo para un salón de clases de Mantenimiento Informático.



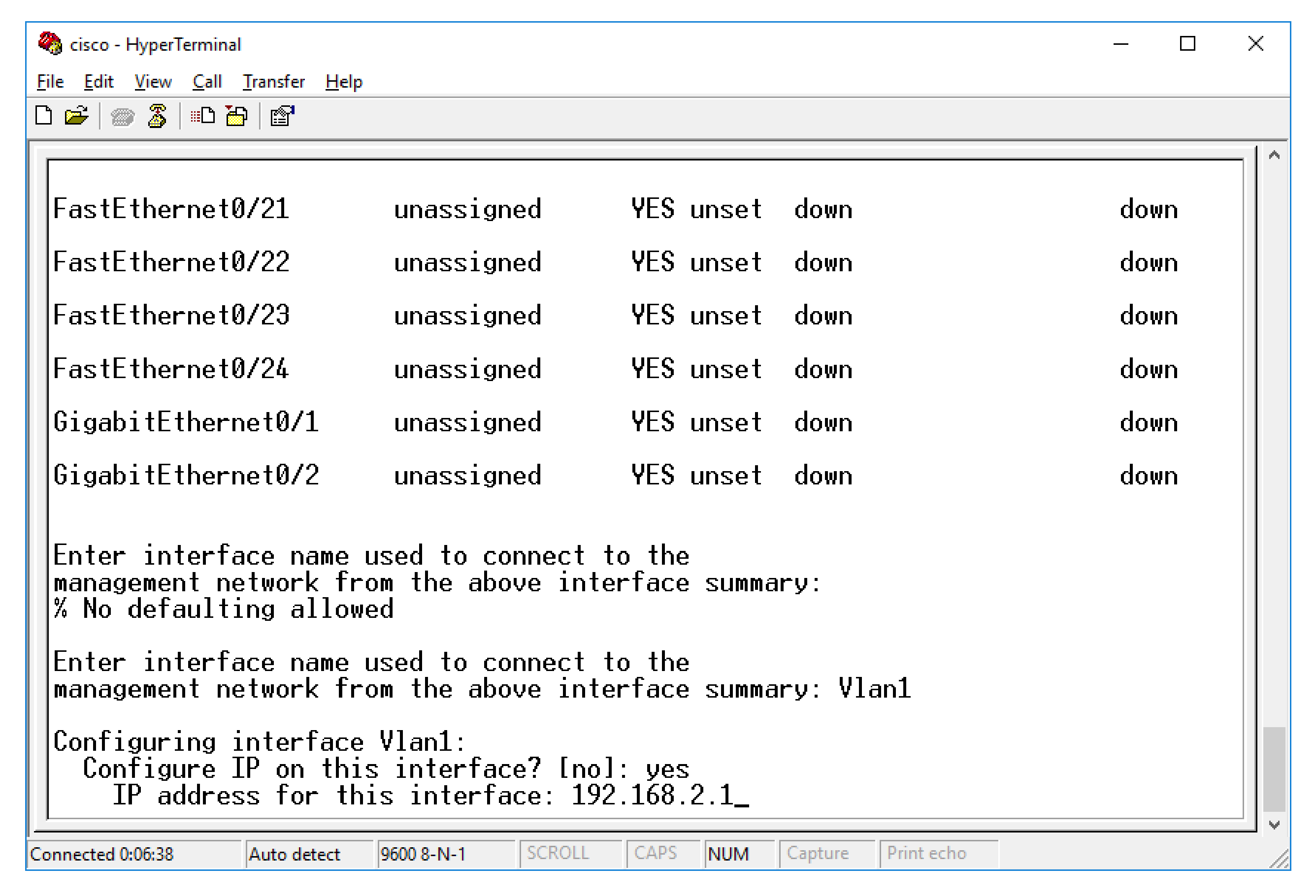

Luego de ingresado el nombre del host, el sistema nos pide que ingresemos la “enable password”, es básicamente la contraseña de usuario que tendremos, vemos en la consola que nos indica que la misma se usa cuando no se ha especificado una clave secreta habilitada “enable secret password” en versiones anteriores del software o imágenes anteriores. En este caso como es la primera vez que inicializamos el switch, recién estamos ingresando ambas contraseñas, las que pueden (o no) ser iguales.

Continuando con el proceso de configuración, el sistema va a mostrar una lista de cada interfaz de red existente en el conmutador y su estado:

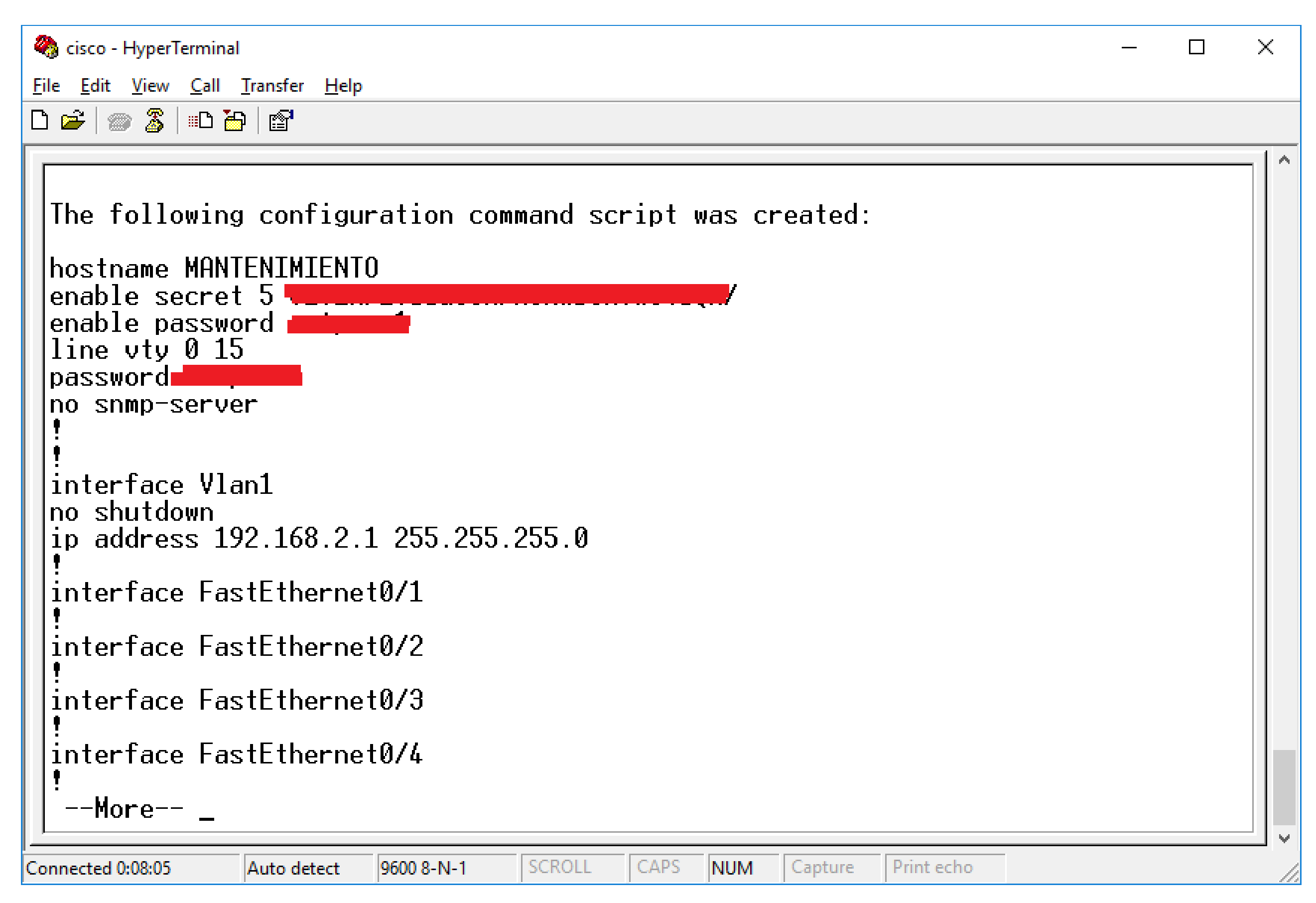



En la primer columna vemos el nombre de cada interfaz, en la segunda su dirección IP (en el momento ninguna está asignada ya que no tenemos ningún equipo conectado y recién estamos configurando el switch), luego indica si está correcta, y su estado (vemos en “up” la interfaz conectada, y en “down” las que aún no hemos conectado).

En la siguiente captura nos dirigimos hasta el final de la lista, y el sistema ya nos pregunta si queremos ingresarle una dirección IP a la lan virtual (Vlan1), e ingresamos para ella la dirección 192.168.2.1:




Una vez realizada la configuración anterior, el sistema muestra un resumen de los cambios hechos:



Nuestro switch ya tiene una configuración básica realizada a través de la terminal, sin embargo, podemos volver a accederlo las veces que sea necesario, por ejemplo para asignar IPs de manera manual a cada interfaz, para crear más redes virtuales, etc. Ya se detalló anteriormente algunos de los comandos básicos para realizar modificaciones en él, pero al tratarse de un conmutador de capa 3, tenemos más posibilidades que pueden explorarse y existe una amplia documentación sobre comandos de configuración a routers y switches Cisco en los manuales oficiales CCNA.

## Subcapa MAC

La capa de Enlace de Datos básicamente se maneja con las direcciones de Hardware (MAC) de los dispositivos, a través de estándares como los anteriormente trabajados (IEEE y Ethernet). Los conmutadores son dispositivos que trabajan con dichos estándares que controlan el acceso al medio y ciertamente existen diferentes mecanismos para controlar la comunicación entre dispositivos.

MAC precisamente en este concepto significa “Media Access Control”, es decir, Control de Acceso al Medio. Los dispositivos pertenecientes a esta subcapa interactúan directamente con el medio físico, y emplean mecanismos de comunicación para permitir que efectivamente un dispositivo emisor y un receptor puedan establecer comunicación. Ya se ha explicado que se localizan mediante direcciones de Hardware, pero ¿Qué tipo de codificación se utiliza para comunicarse? Como se mencionó en el apartado de comunicación de esta guía, la comunicación puede ser síncrona o asíncrona. Como ejemplo de comunicación síncrona, tenemos algoritmos de codificación que permiten coordinar los bits enviados con pulsos de reloj, de ese modo un equipo puede enviar un mensaje sincronizado en el tiempo y el equipo receptor podrá interpretarlo sin inconvenientes. La codificación Manchester es un ejemplo de mecanismo para este fin.

### *Codificación Binaria directa*

Conceptualmente, codificación binaria directa implica que a través de un período de tiempo controlado por pulsos de reloj, se haga corresponder una señal sin tensión para representar un 0, y una tensión de 5 voltios para representar un 1. Por cada pulso del reloj el receptor interpretaría un 1 en caso de recibir corriente eléctrica y 0 en caso contrario. No obstante, esto lleva a grandes ambigüedades debido a que puede confundirse un bit 0 con un bit neutro, confundiendo un 0 bit de un emisor con un emisor inactivo que lógicamente también está enviando 0v de tensión.

Este problema podría solucionarse utilizando una tensión de 1v para representar un 1 binario y -1v para representar un 0, no obstante ninguno de los estándares de Ethernet pueden implementar esto ya que con esta última solución, un receptor podría muestrear una señal a una frecuencia ligeramente diferente a la que la ha enviado el emisor para generarla, las diferentes velocidades del reloj podrían producir asincronía respecto a donde están los límites de los bits, sobre todo si tenemos una cadena larga de 0s consecutivos seguida de una cadena de 1s consecutivos.

Existen otros estándares de codificación que sí son utilizados por Ethernet, como ser la codificación Manchester y la codificación Manchester diferencial.

### *Codificación Manchester*

*En la codificación Manchester, cada periodo de bit se divide en dos intervalos iguales. Un bit 1 binario se envía teniendo el voltaje alto durante el primer intervalo y bajo durante el segundo. Un 0 binario es justo lo inverso: primero bajo y después alto. Este esquema asegura que cada periodo de bit tenga una transición a la mitad, facilitando que el receptor se sincronice con el emisor. Una desventaja de la codificación Manchester es que requiere el doble de ancho de banda que la codificación binaria directa, pues los pulsos son de la mitad de ancho. Por ejemplo, para enviar datos a 10 Mbps, la señal tiene que cambiar 20 millones de veces/seg. La codificación Manchester se muestra en la figura 4-16(b).*

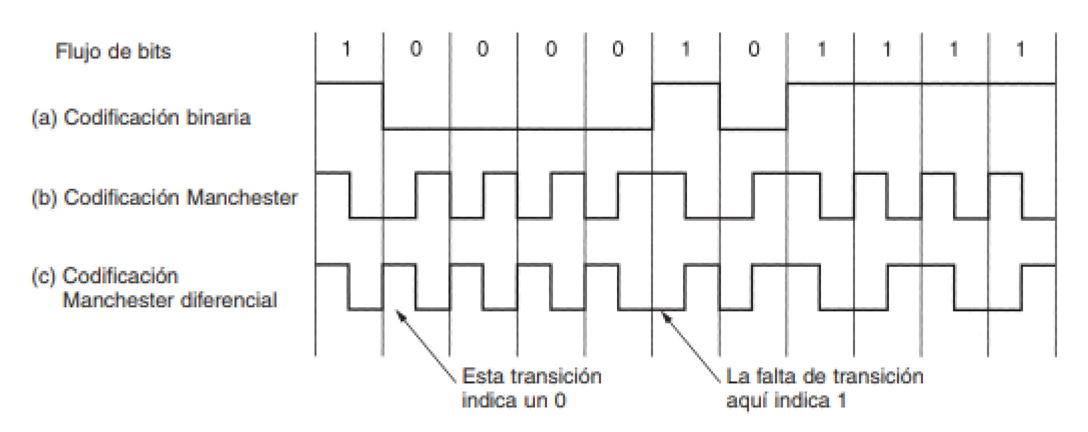



**Figura 4-16.** (a) Codificación binaria. (b) Codificación Manchester. (c) Codificación Manchester diferencial.

(Tanembaum, 2014).

### *Codificación Manchester Diferencial*

La codificación Manchester diferencial, que también puede verse en la figura anterior, es una variación de la codificación Manchester básica. En ella, un bit 1 se indica mediante la ausencia de una transición al inicio del intervalo. Un bit 0 se indica mediante la presencia de una transición al inicio del intervalo. En ambos casos también hay una transición a la mitad.

Para implementar el esquema diferencial se necesita un equipo más complejo, pero se ofrece mayor inmunidad ante el ruido. Todos los sistemas Ethernet usan codificación Manchester debido a su sencillez. La señal alta es de + 0.85 voltios, y la señal baja es de − 0.85 voltios, dando un valor de corriente continua de 0 voltios.

Ethernet no utiliza la codificación Manchester diferencial, pero otras LANs si lo emplean, un ejemplo de ello es la Token Ring 802.5. El estándar “Token Ring” era un sistema utilizado en redes con topología de anillo, donde una trama de 3Bytes viajaba por todos los equipos, y se le llamaba “token”. Se utilizó ampliamente en la década de 1970s y en su estándar 802.5 llegaba a velocidades de 4 o 16 Mbps, pero en la actualizad se encuentra en desuso por la popularidad y velocidad del estándar Ethernet.

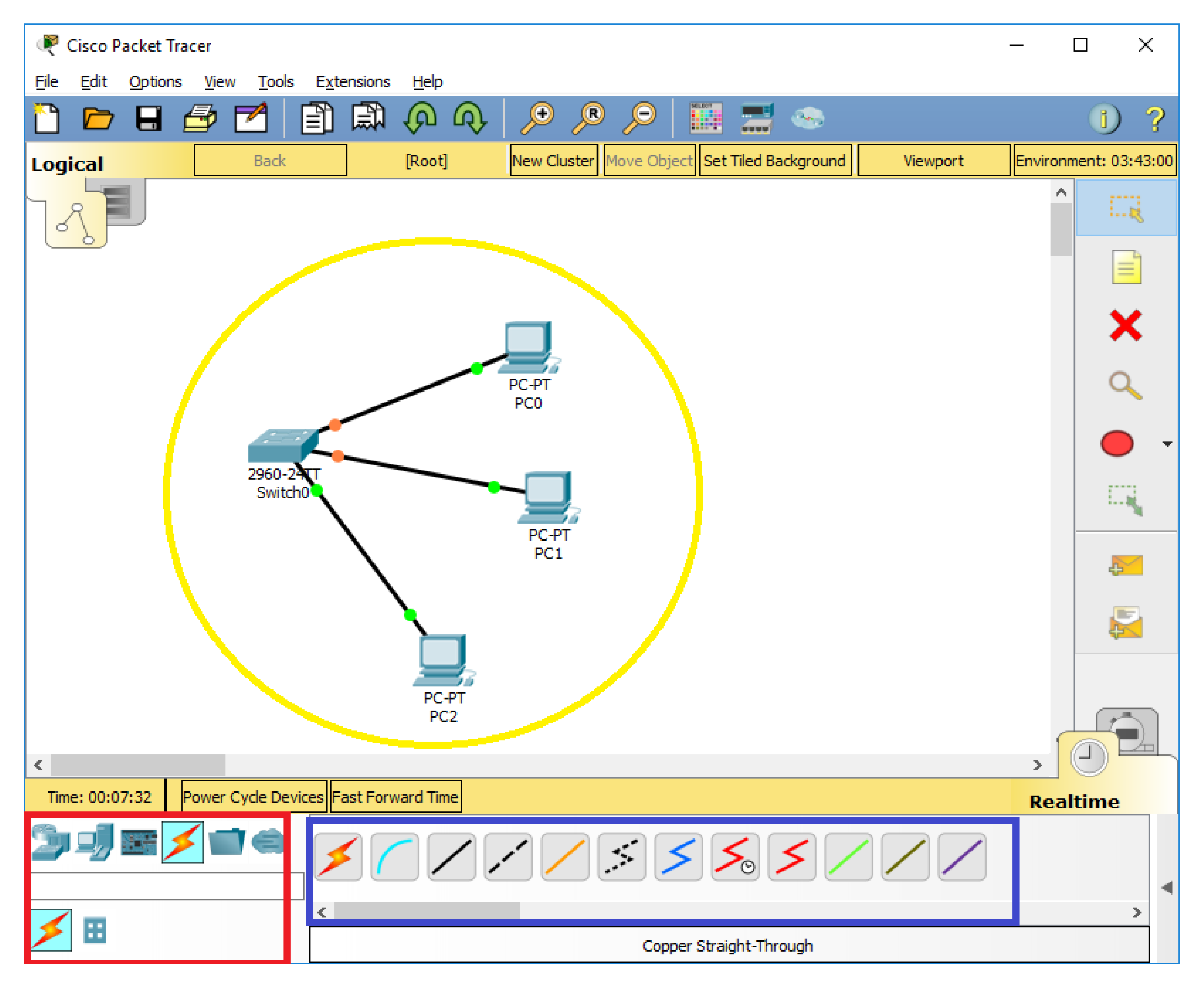
## Practicando contenidos de la unidad: Visualización de tramas Ethernet y dominios de difusión

Para poner en práctica los contenidos anteriores y visualizar cómo se envían las tramas Ethernet en una red podemos utilizar un Software que emule una red real, y permita visualizar el encaminamiento y composición de las tramas. La compañía Cisco Systems desarrolló la aplicación **Packet Tracer**, en la misma son soportadas una amplia multiplicidad de protocolos que permiten a los estudiantes experimentar con una red sin necesidad de necesitar una red real, y observar el funcionamiento interno de los paquetes, lo que no podrían hacer dentro de una red en producción.

### *Uso del software CISCO Packet Tracer*

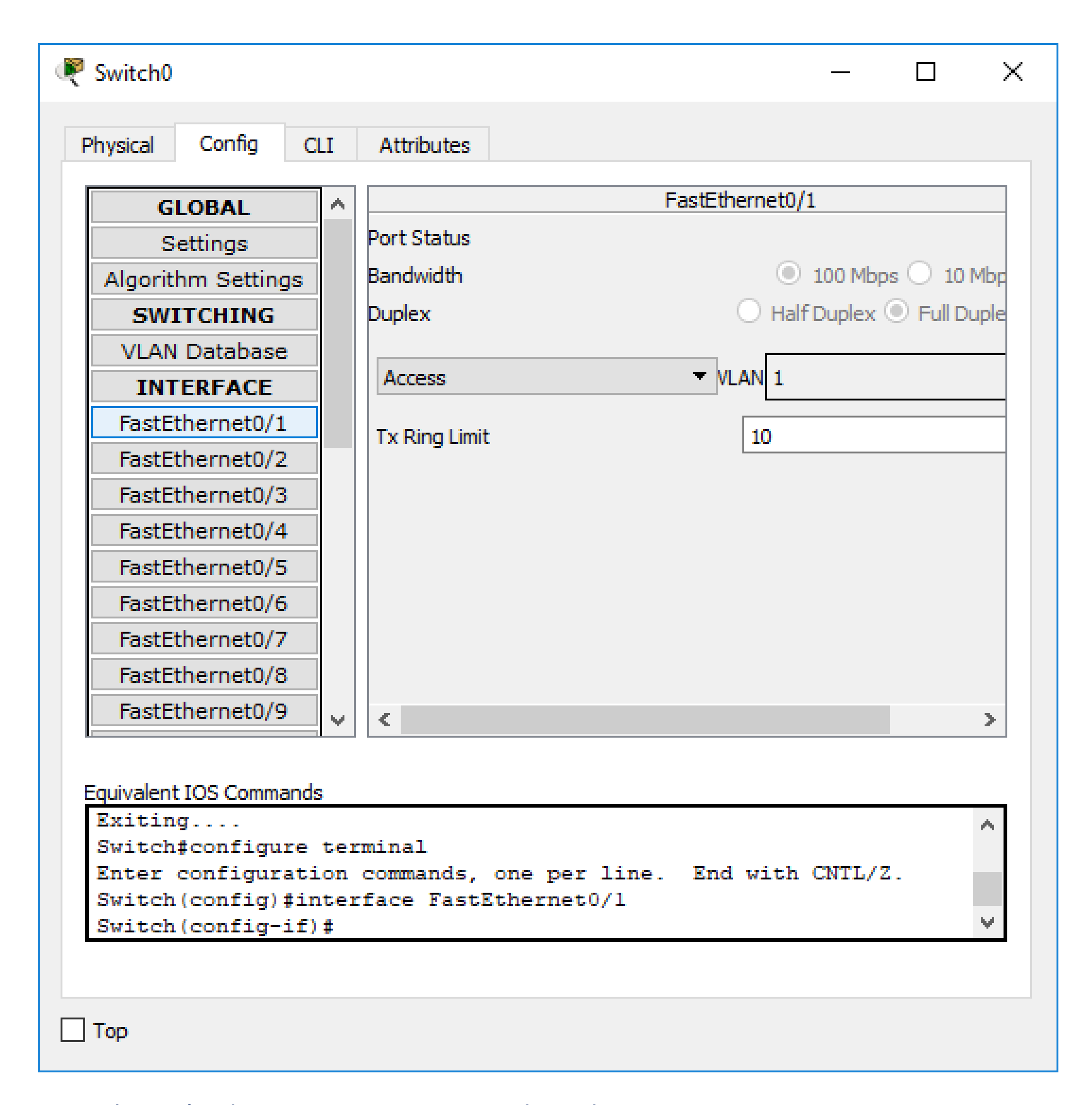
En primer lugar debemos descargarnos el programa e Instalarlo, su distribución es libre por lo cual el lector podrá obtenerlo sin dificultad. No se colocarán links en esta guía puesto a que si se lo hiciera, a futuro los enlaces podrían ya no ser válidos, y es una aplicación cuyo acceso es muy sencillo y se asume que el usuario no tendrá problemas para obtenerla. La versión que se utilizará para este caso es la más reciente en este momento, que es la 7.1.1. Debemos tener una cuenta en el sitio de Cisco Network Academy para poder acceder al software como estudiante autentificado de Cisco, no obstante, podemos probar sus funcionalidades como invitado, cliqueando sobre “Guest Login” al iniciar la aplicación.

En la siguiente imagen, podemos ver un esquema de red extremadamente básico que se ha colocado, utilizando como caso de ejemplo tres computadoras terminales conectadas por cable par trenzado a un switch 2960. No obstante, el sistema permite emular sistemas mucho más complejos, esquemas de redes complejos emulando dispositivos de muy alto costo como ser routers de todos los modelos de Cisco, por conectores de todos los tipos y dispositivos conectados a la red de diversa índole, como ser interruptores, sensores de detección de humo, de humedad, genéricos y un largo etcétera.




Señalizados en amarillo podemos ver el esquema de red colocado actualmente, simplemente arrastrando con el mouse desde el panel inferior de dispositivos hasta el área principal. Señalizados en rojo tenemos un panel de dispositivos entre los cuales podemos seleccionar a nuestro antojo una amplia variedad de dispositivos de red, conectores y otros equipos. En el panel señalizado en azul se ven las variedades para el tipo de equipo seleccionado en el panel anterior. Para el caso anterior se seleccionaron "conectores" y a la izquierda vemos que existen conectores de consola, cable directo, cruzado, fibra óptica, etc.

Si hacemos doble clic sobre cualquier dispositivo esquematizado en la red podemos configurar sus características de hardware, en el caso del switch por ejemplo tenemos una primer pestaña con su configuración física, y en la segunda pestaña mostrada en la siguiente imagen, se puede ver su configuración interna, las VLANs, y la configuración de cada interface de red. En el panel inferior se ven los comandos equivalentes que deberíamos colocar en un switch real para efectuar las mismas configuraciones desde los comandos de IOS:

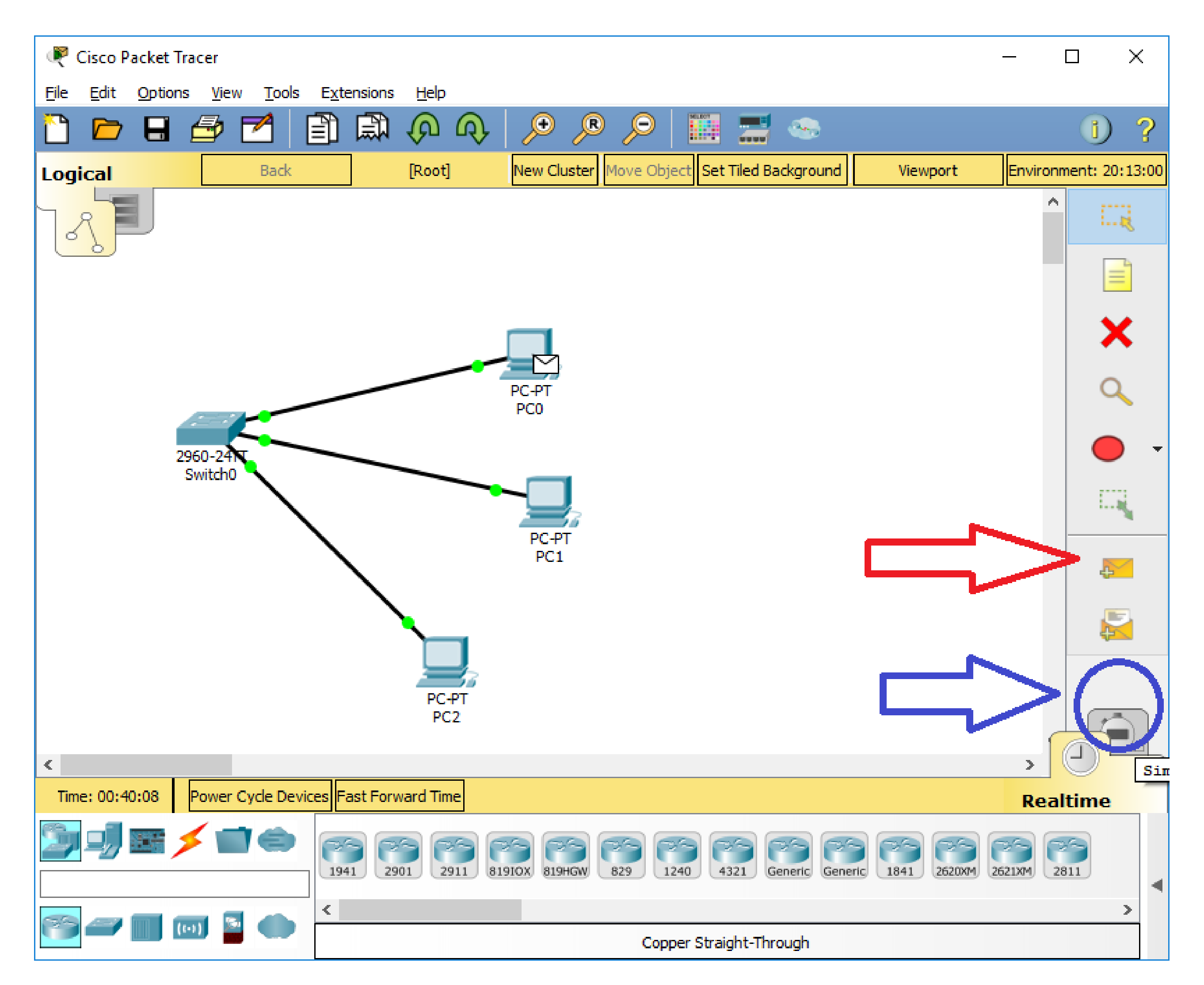



### *Visualización de tramas y paquetes de red*

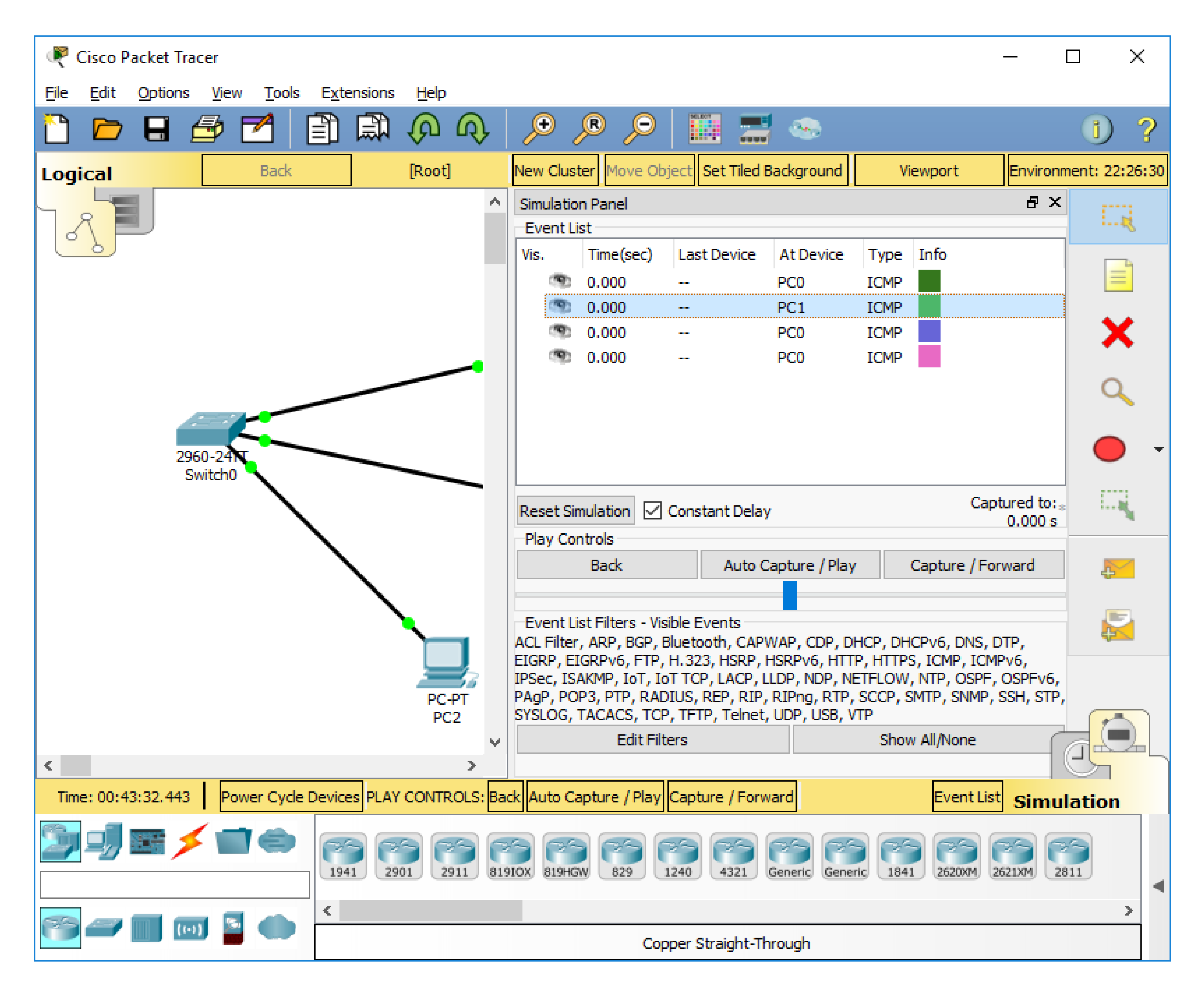
Para que exista efectivamente una red simulada y poder enviar paquetes entre equipos, debemos configurar las IPs de los equipos para que se encuentren dentro de una misma VLAN. Podremos visualizar también qué protocolos intervienen en el envío de paquetes y por donde pasan desde la vista de simulación.

- Debemos configurar para ello las interfaces del switch como activadas.
- A cada equipo para el caso de ejemplo le asignaremos IPs estáticas (puesto a que no estamos utilizando un router ni servicios DHCP).
- La IP de Gateway, es decir, la puerta de enlace predeterminada de cada equipo será la 192.168.1.1, mientras que los equipos de arriba hacia abajo los configuraremos con las IP 192.168.1.2 hasta la 192.168.1.3.

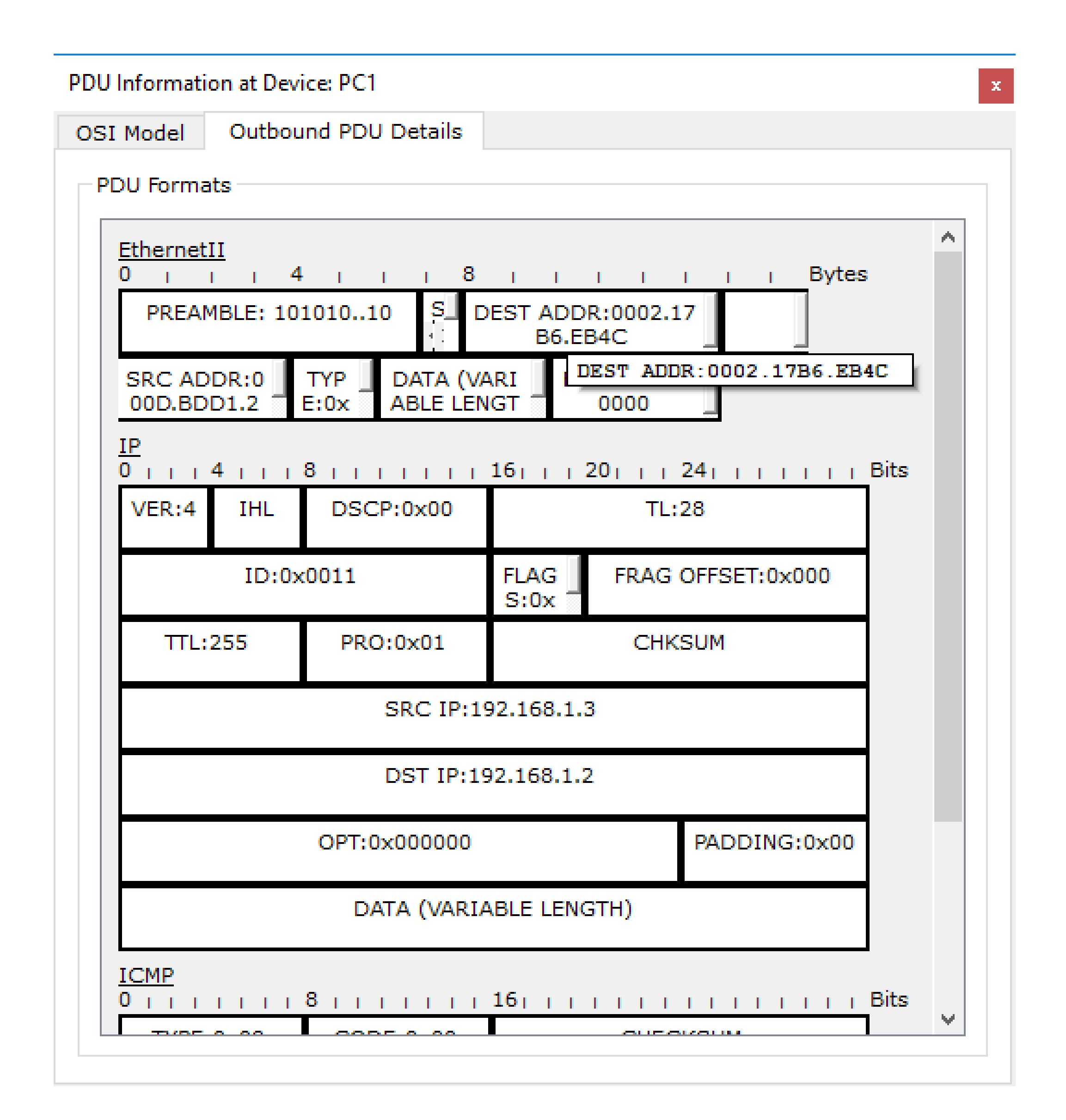
Luego de realizada esta configuración básica, simularemos el envío de un paquete utilizando la función señalizada en rojo , mientras que la vista en tiempo real debe accederse desde la opción señalizada en azul:




Desde la vista en tiempo real, pueden verse todos los paquetes colocados a través de los protocolos (en este caso de estudio ICMP), como se ve en la siguiente imagen:




Si hacemos doble clic sobre el paquete podemos observar todas sus características internas en la capa correspondiente. En la ventana emergente debemos seleccionar la pestaña de los detalles salientes del paquete “Outbound PDO details” y si queremos ver cómo está compuesta una trama debemos observar su estado de capa 2, desde donde se ven el preámbulo, las direcciones de hardware de origen y destino, el FCS, así como también los detalles del paquete en capa de red y detalles específicos del paquete, en nuestro caso referidos a su protocolo ICMP. En la ventana emergente debemos seleccionar la pestaña de los detalles salientes del paquete “Outbound PDO details”. En la imagen puede verse esta información:




### *Puerta de enlace predeterminada y dirección de Broadcast*

Ahora que ya hemos trabajado en secciones anteriores cómo crear una pequeña red local (ver Crear una pequeña red local entre dos o varios equipos), que hemos implementado también en el Packet Tracer pequeñas redes para ver qué forma toman las tramas y paquetes en la red, cabe señalar un par de definiciones importantes con las que es seguro que nos hayamos topado cada vez que configuramos manualmente la IP de un equipo. Éstos son, la puerta de enlace predeterminada que le asignamos, y la dirección de broadcast o difusión:

Puerta de Enlace Predeterminada (Gateway):

Es el dispositivo que permite que dos o más redes se encuentren interconectadas, es decir, permite que exista tráfico de datos entre varias redes diferentes. Este equipo, que puede ser una computadora o un enrutador, tiene asignada generalmente la primer dirección IP de nuestra subred.

Hasta el momento, lo más usual que encontramos es configurar una LAN con varios equipos conectados a un enrutador, y ese enrutador a su vez conectado a Internet, suministrando salida a Internet para cada computadora, dicho equipo en cuestión, es el Gateway o puerta de enlace, ya que permite conectar nuestra red local con el resto de la red global.

Ejemplo:

- *Tenemos una LAN con 4 equipos que toman las direcciones IP 192.168.1.2, 192.168.1.3, 192.168.1.4 y 192.168.1.5; entonces la puerta de enlace predeterminada, en este caso hipotético un enrutador, tendrá la IP 192.168.1.1.*

Dominio de Difusión (Broadcast):

La palabra *broadcast* ya nos hace referencia a transmisión, por lo que podemos imaginar su significado en el ámbito de las redes. El dominio de difusión es el área lógica en el cual una computadora conectada en red puede trasmitir datos a cualquier otra computadora dentro de la misma subred sin necesidad de un dispositivo que encamine esos datos (como un router). Al no necesitar un equipo que se encargue del encaminamiento de datos, se deduce que este dominio sólo es válido dentro de una misma subred, red LAN o VLAN donde cada equipo tiene acceso directo a otros equipos a través de su dirección IP local, que comparten el mismo rango de IPs y la misma puerta de enlace predeterminada.

La dirección IP que se le asigna al dominio de difusión será la última dirección IP de la subred. En el ejemplo anterior, si tenemos una LAN con 4 equipos conectados a un router, y éste tiene la IP 192.168.1.1, suponiendo que la máscara de subred es 255.255.255.0, la dirección de Broadcast será 192.168.1.255.

*Nota: De lo esbozado anteriormente obsérvese que las direcciones IP efectivas que pueden tomar las computadoras en una red van desde la segunda dirección (ej: 192.168.1.1) hasta la pen última (ej: 192.168.1.254), ya que la primera está reservada para la red y la última para el Broadcast. Además de esto, tenemos una IP adicional que es ocupada por el equipo que funciona como Gateway, por lo general, la primera de las direcciones efectivas.*

# Capa de Red

Anteriormente ya hemos trabajado con las dos capas inferiores del modelo OSI, en primer lugar trabajamos con la capa física y sus conceptos fundamentales respecto a las señales que se transmiten en el medio físico a través de flujos de bits, posteriormente se trabajó con la capa de enlace de datos, que controla el acceso al medio físico y encapsula la información en tramas de datos, donde la dirección de Hardware (MAC) de cada equipo jugaba un rol fundamental. Ahora es tiempo de trabajar con la capa de RED, la cual desarrollaremos más adelante, pero podemos anticipar muy brevemente que se encarga de todo el direccionamiento lógico entre equipos, el enrutamiento, encapsulamiento de datos y disencapsulamiento.

La función principal de esta capa, es transferir los datos desde el equipo que los origina hasta un equipo receptor pasando por varias redes intermedias si fueran necesarios.

## Protocolos de capa de Red:

Son varios los protocolos que intervienen en esta capa, básicamente todos aquellos que se encarguen del direccionamiento a través de IP pertenecen a esta capa, a saber, IP, ICMP, ARP, RARP, RIP y OSPF son todos protocolos de capa de red. Algunos de ellos ya los hemos mencionado anteriormente y ahora los trabajaremos en profundidad, otros conceptos debemos empezar a definirlos. Sin embargo, subyace que el protocolo más importante en capa de Red es el protocolo IP, el cual tiene 2 versiones existentes:

### Protocolo de Internet Versión 4 (IPv4)

Bajo este protocolo nació lo que actualmente conocemos por Internet, consiste en que cada equipo de la red tome una dirección de 32 bits, separadas en 4 octetos (números de 8 bits) expresadas con notación decimal. Así, para cada octeto podemos representar números de entre el 0 y 255.

Todas las IP presentadas en ejemplos anteriores son IPv4, como por ejemplo 10.0.0.1 o 192.168.10.2.

**El problema** evidente que ofrece este tipo de direccionamiento es obvio, y es que la cantidad de direcciones que pueden existir es muy limitada, si tenemos 256 posibilidades para cada octeto, tenemos 256*256*256*256 posibles direcciones IP en total, lo que llevaría a direccionar hasta 4.294.967.296 equipos, y si la cantidad de personas que habitan el planeta es bastante mayor a ese número, ¡Vaya si la cantidad de equipos conectados a Internet lo exceden!. Lo cierto es, que existen mucho más dispositivos conectados a la red en diferentes subredes que la cantidad de IPv4 existentes, por lo que sería imposible que se asigne una sola IP, única e irrepetible a cada dispositivo conectado a Internet.

**La solución** hasta el momento ha sido crear sistemas de direccionamiento con IPs públicas y privadas, donde en Internet existen servidores que toman una sola IPv4 única e irrepetible, pero conectan a su vez muchas redes. Estos servidores toman lo que se conocen como IPs públicas, mientras que las subredes conectadas a éstos pueden manejar internamente otras direcciones IP para sus equipos, incompatibles entre sí, pero

válidas dentro de cada red local, estas direcciones son las llamadas IPs privadas, y los equipos de diferentes subredes pueden interconectarse empleando un mecanismo conocido como NAT (Network Adress Translation -traductor de direcciones de red-). Más adelante se desarrollará sobre el funcionamiento de éste mecanismo.

## Protocolo de Internet Versión 6 (IPv6)

En IPv6 se utiliza la misma lógica anterior, pero en lugar de trabajar con direcciones de 32 Bits se trabaja con direcciones de 128 Bits. La cantidad de combinaciones de direcciones aquí eliminaría el problema anterior, tenemos $2^{128}$ direcciones IPv6 totales. Se expresan en 8 secciones de 16 Bits, separadas por dos puntos ":". En cada sección, tenemos entonces 65.536 posibles combinaciones, entonces la cantidad de IPs posibles es 65.536 elevado a la 8.

Para facilitar su manejo, se expresa cada sección en hexadecimal (16 diferentes caracteres del 0 al 9 y de la "a" a la "f"). Un ejemplo de dirección IPv6 es:

2557 : ac0f : 4 : 2117 : a910 : 15 : ae2f : 102b

IPv6 ya existe y se implementa, no se trata de una tecnología futurista, simplemente que su uso en Internet no se ha extendido y aún en la actualidad se emplean direcciones IPv4 debido a que mudarse a IPv6 conllevaría a una inversión extremadamente alta en infraestructura, cambiando dispositivos de hardware y mano de obra de millones de personas para migrar todos los servicios actuales a la tecnología IPv6. Es un cambio que dejaría atrás toda la problemática del direccionamiento IPv4, que hasta ahora no se ha realizado, pero es posible que en algún momento se haga necesario.

## Redes Privadas

Todas las redes LAN que hemos ejemplificado anteriormente son privadas, puesto que cada equipo utiliza direcciones IP locales (o privadas) que son útiles para comunicarse entre sí, pero si a la red le colocamos salida a Internet, entonces dicha dirección no será válida en la red de redes, únicamente sirve para la transmisión de datos dentro de la misma red interna, las IPs que usualmente utilizan las redes privadas para sus equipos son del estilo 192.168.x.x o 10.x.x.x y son todas reservadas como privadas.

*"En Internet, una **red privada** es una red de computadoras que usa el espacio de direcciones IP especificadas en el documento RFC 1918. A los equipos o terminales puede asignárseles direcciones de este espacio cuando deban comunicarse con otros terminales dentro de la red interna/privada (una que no sea parte de Internet/red pública) pero no con Internet directamente.*

*Las redes privadas son bastante comunes en esquemas de redes de área local (LAN) de oficinas, empresas y ámbito doméstico, debido a que no tienen la necesidad de usar direcciones IP públicas es sus dispositivos (PC, impresora, etcétera), compartiendo todos los dispositivos de la red privada la misma dirección pública, habitualmente la del módem del router."* *(Wikipedia)*

## Direccionamiento Global y tecnología NAT

Ya se ha especificado que existen direcciones IPs que están reservadas para redes privadas y que no se utilizan en Internet, las mismas se encuentran especificadas

en el documento RFC 1918 [(ver)](), sin embargo, cabe destacar que hay equipos que sí tienen una IPv4 fija en Internet y que permiten ser identificados desde cualquier otra computadora conectada, dichos equipos toman direcciones que conocemos como IPs públicas, y generalmente son empleados por los servidores y grandes enrutadores de las compañías telefónicas. Se utilizan protocolos de enrutamiento para su interconexión, y permiten que equipos de diferentes subredes puedan intercambiar información entre sí.

Las direcciones IP públicas globales se encuentran reguladas por la Internet Assigned Numbers Authority (se conoce con su acrónimo, IANA), la cual es una entidad que regula los servidores raíz de nombres de dominio DNS, sistemas autónomos y direccionamiento IP global, actualmente es un departamento operado por la ICANN (Corporación de Internet para la Asignación de Nombres y Números), organización que se encuentra en el Estado de California (USA) y se encuentra a su vez sujeta a las leyes de dicho Estado.

### *Direcciones IP públicas*

Las direcciones IP públicas son las direcciones IP que la IANA habilita a nuestro proveedor de servicios de internet (ISP) y efectivamente, es único en Internet. Cuando nos conectamos a Internet, a nuestra computadora se le asigna una IP pública a través de la cual los otros dispositivos de Internet pueden comunicar, y desde la cual se identifica el tráfico saliente de nuestra computadora. Nuestro ISP utilizará una dirección IP pública fija, y a su vez asignará a cada equipo conectado a Internet direcciones IP públicas dinámicas; esto es, que una vez que el equipo se desconecte de Internet (o se apague), en el momento de establecer nuevamente conexión, la ISP le asignará una dirección IP pública diferente.

En el siguiente esquema se ilustra la relación entre direcciones IPs públicas y privadas:

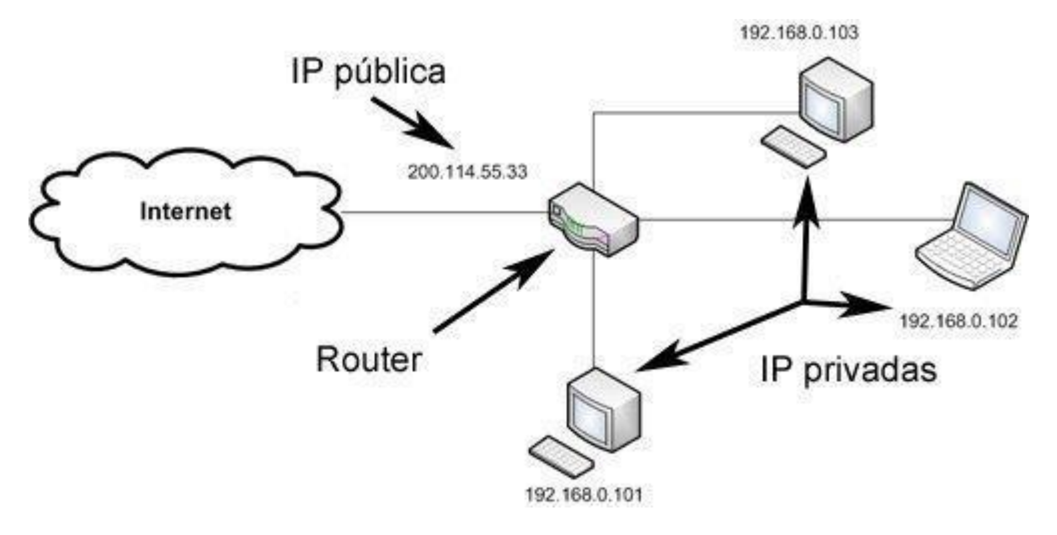



*Imagen obtenida de [HostInet]()*

### *Direcciones IP privadas*

Como se ilustra en el esquema anterior y se ha explicado anteriormente sobre Redes privadas, las direcciones IP privadas son aquellas con las cuales nuestro equipo se identifica dentro de la misma subred o red LAN. Los servidores de Internet no utilizan direcciones IP con ese formato, son los equipos locales los que se comunican con esas direcciones y son accedidas entre sí por un conmutador o enrutador, este dispositivo,

puede estar conectado a un módem ADSL para la salida a Internet, cuya IP publica sí es asignada por la ISP, generalmente de manera dinámica.

Si tenemos el ejemplo anterior, la IP pública 200.114.55.33 para Internet, todos los equipos conectados a ese router se identificarán bajo la misma IP, sin embargo a nivel de la red local, los equipos toman las IPs 192.168.0.101 a la 192.168.0.103 (privadas).

### *IP Fija o Estática*

Podemos asignar en una red local direcciones IP fijas a nuestros equipos, pero estamos hablando aquí de direcciones privadas siempre. En la red pública, las IP fijas son la que utiliza nuestro ISP o bien, son usadas por proveedores de servicios web, los grandes servidores por ejemplo deben contratar direcciones de IP públicas fijas, y el rango que pueden tomar varía en diferentes países. También se pueden contratar de manera particular direcciones públicas fijas, pero esa inversión no tendría sentido de no ser para una empresa de considerables dimensiones o para servidores web.

### *IP Dinámica*

Habitualmente los proveedores de Internet ofrecen direcciones de IP dinámicas para sus clientes, esto permite reducir el gasto de direcciones y reutilizar las direcciones IPs entre diferentes equipos. Cuando un equipo se desconecta, simplemente pierde la dirección IP antes asignada y adquiere otra IP cuando se reconecta. Para asignar IPs públicas a pequeñas empresas, oficinas y hogares generalmente éste es el mecanismo que utilizan las ISP, ya que las IP fijas deben contratarse explícitamente por el cliente y obviamente tiene otro costo.

### *Traducción de direcciones de red (NAT)*

Anteriormente ya se ha mencionado que el mecanismo que permite que exista conexión entre dispositivos de diferentes subredes se conoce como NAT, ya que es posible que entre dos subredes diferentes se usen las mismas IPs privadas a sus respectivos equipos, o que el rango de IP que manejen sea completamente incompatible, y sin embargo, la tecnología NAT permite que exista comunicación entre sus equipos:

*"La traducción de direcciones de red o NAT (del inglés Network Address Translation) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo. (…)*
*NAT es como el recepcionista de una oficina grande. Imagine que le indica al recepcionista que no le pase ninguna llamada a menos que se lo solicite. Más tarde, llama a un posible cliente y le deja un mensaje para que le devuelva la llamada. A continuación, le informa al recepcionista que está esperando una llamada de este cliente y le solicita que le pase la llamada a su teléfono.*

*El cliente llama al número principal de la oficina, que es el único número que el cliente conoce. Cuando el cliente informa al recepcionista a quién está buscando, el recepcionista se fija en una tabla de búsqueda que indica cuál es el número de extensión de su oficina. El recepcionista sabe que el usuario había solicitado esta llamada, de manera que la reenvía a su extensión.*

***Nat. Estática***

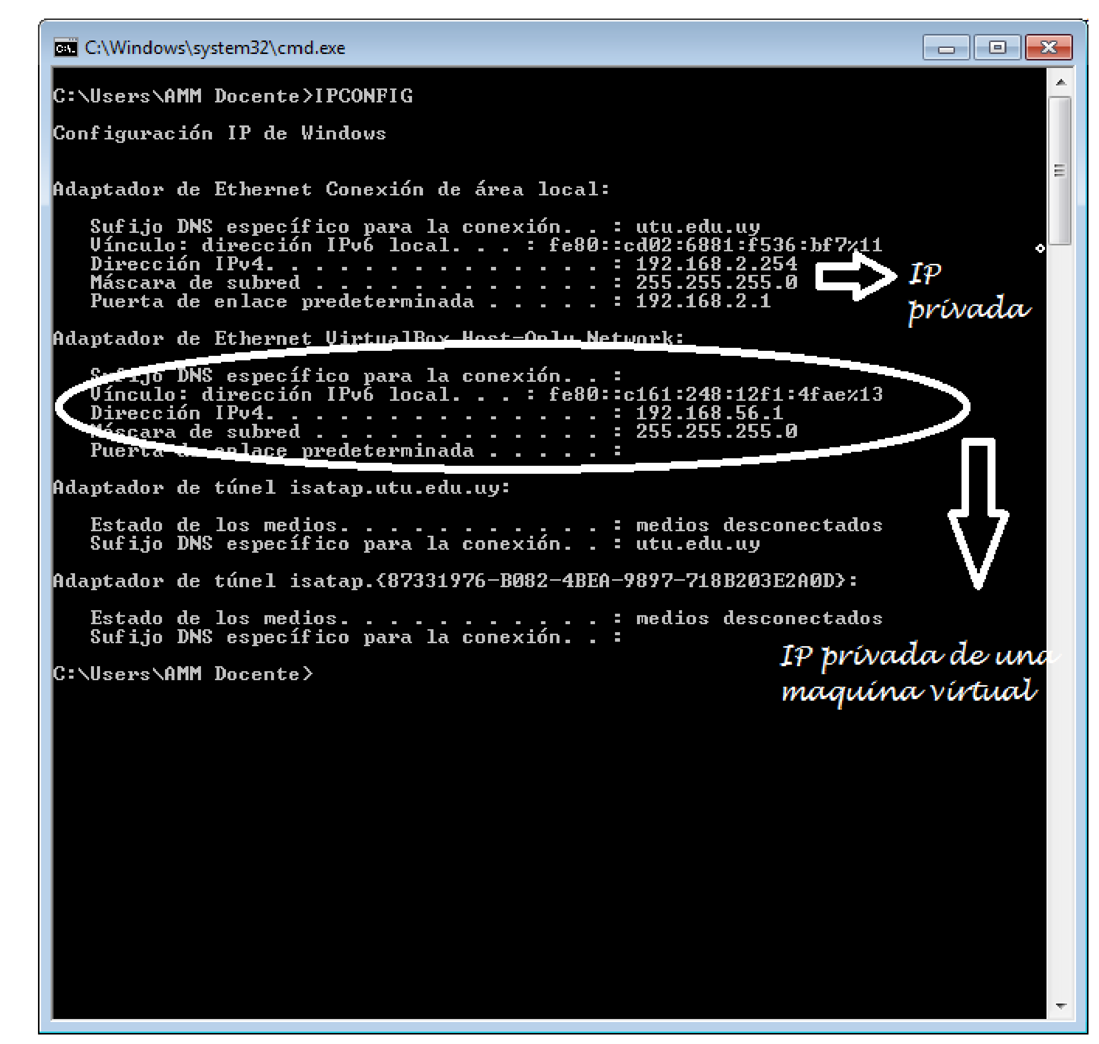
*Conocida también como NAT 1:1, es un tipo de NAT en el que una dirección IP privada se traduce a una dirección IP pública, y donde esa dirección pública es siempre la misma. Esto le permite a un host, como un servidor Web, el tener una dirección IP de red privada pero aun así ser visible en Internet.*

***Dinámica***

*Es un tipo de NAT en la que una dirección IP privada se mapea a una IP pública basándose en una tabla de direcciones de IP registradas (públicas). Normalmente, el router NAT en una red mantendrá una tabla de direcciones IP registradas, y cuando una IP privada requiera acceso a Internet, el router elegirá una dirección IP de la tabla que no esté siendo usada por otra IP privada. Esto permite aumentar la seguridad de una red dado que enmascara la configuración interna de una red privada, lo que dificulta a los hosts externos de la red el poder ingresar a ésta. Para este método se requiere que todos los hosts de la red privada que deseen conectarse a la red pública posean al menos una IP pública asociadas.''* (Wikipedia)

## Poniendo en práctica algunos contenidos…

Es momento de practicar un poco los contenidos anteriormente trabajados sobre direcciones IP públicas y privadas. Desde una consola de comandos (CMD en Windows) o una terminal si utilizamos Linux debemos tipear un comando para verificar la dirección de nuestra computadora, en Windows el comando es *ipconfig* mientras que en Linux es *ifconfig.* En el equipo desde el cual se está escribiendo en este momento, se obtiene el siguiente resultado:

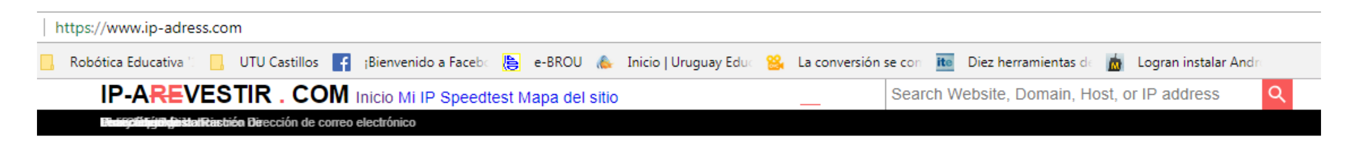



Como podemos ver, el equipo tiene la IP 192.168.2.254, la cual claramente es una IP privada, es decir, es la IP con la cual lo identifican otros equipos de la subred.

La información que aparece sobre el adaptador de Ethernet de VirtualBox corresponde a una máquina virtual que tenemos instalada en este caso, cuya IP es una dirección lógica de una tarjeta de red que es emulada por software. No trabajaremos con ella en este apartado. Practicar estos conceptos requieren de la instalación de máquinas virtuales y su configuración dentro de la red existente, no es propósito de esta guía desarrollar sobre eso,ya que requiere más que nada de la práctica por parte del lector, el cual puede simular redes locales enteras y computadoras enteras a través de un software de virtualización, utilizando una única computadora personal.

### *¿y cómo sé cuál es mi IP pública?*

Existen sitios web con aplicaciones específicas para conocer nuestra IP y algunos detalles sobre nuestra ISP, una de ellas es ip-adress.com, que cuando entramos desde el equipo actual como ejemplo nos dice que en este momento nuestra IP es 190.0.150.3, y además identifica dicha IP con la ISP de ANTEL que se encuentra en Uruguay:




¿Cuál es mi dirección IP? Su dirección IP es: **190.0.150.3**

Bienvenido a IP-Adress.com, donde puede determinar rápida y fácilmente su dirección IP o obtener más información sobre un dominio o nombre de host.
La dirección de su dirección IP es *Uruguay* y el ISP de su dirección IP es *Administración Nacional de Telecomunicaciones* . Obtenga más información sobre su dirección IP en la página Mi IP ...

## Clases de Direcciones IP

Anteriormente hemos trabajado con conceptos bien importantes y claves para comprender la utilidad de la capa de red, en particular relacionado el protocolo IP en sus diferentes versiones, y se han mostrado ejemplos de configuración de equipos asignando su IP y máscara de subred, además se habló de direcciones de Red, Gateway y de Broadcast y se diferenció direcciones IP estáticas de dinámicas.

Ahora es momento de hablar de las diferentes clases de direcciones IP y de las diferentes redes que pueden crearse dentro de una red ya existente, dependiendo de la clase a la cual dicha red pertenezca. Se habló anteriormente de que una IP dinámica es asignada por el servicio DHCP de un servidor o enrutador cuando un equipo (host) se conecta a la red; al desconectarse, pierde esa dirección IP y al reconectarse se le asigna otra. La nueva dirección IP tendrá algo en común con respecto a la que antes tenía: Pertenece a la misma subred, es decir, se encontrará bajo el mismo rango de direcciones IP permitidas por el servidor dependiendo de la máscara y dirección IP que tenga configurado.

Las direcciones asignadas por un servidor dentro de una subred siempre pertenecerán a la misma clase. **Una clase de direcciones IP, es precisamente una división jerárquica que posee el protocolo para poder clasificar las direcciones dependiendo de la finalidad de la red a la que pertenezca para poder garantizar la eficiencia atendiendo a las necesidades de los hosts.**

Existen cinco clases diferentes de IP, y las podemos identificar a través de su primer octeto:

- **Clase A:** Comprende las direcciones que van desde la 0.0.0.0 hasta la 127.255.255.255 y se utiliza exclusivamente para redes de gran dimensión. Cabe destacar aquí, que la mitad de las direcciones IP disponibles pertenecen a esta clase, no obstante, no todas las direcciones son válidas, ya que muchas de ellas son reservadas, por ejemplo, la primer dirección corresponde a la IP por defecto, y las que corresponden a la forma 127.x.x.x pertenecen a direcciones de loopback (direcciones hacia el mismo equipo), reduciendo la cantidad de IPs efectivas.

- **Clase B:** Contiene las direcciones IP comprendidas entre la 128.0.0.0 hasta la 191.255.255.255 y son utilizadas para redes medianas.
- **Clase C:** Contiene las direcciones IP comprendidas entre la 192.0.0.0 hasta la 223.255.255.255 y se emplea en redes pequeñas. Es la clase de direccionamiento que generalmente se utiliza en redes LAN.
- **Clase D:** Corresponde a las IP comprendidas entre la 224.0.0.0 hasta la 239.255.255.255 y se utilizan para servicios de Multicasting (multidifusión) que implica que múltiples redes pueden enviar información a múltiples destinos de manera simultánea.
- **Clase E:** Corresponde a las direcciones comprendidas entre la 240.0.0.0 hasta la 255.255.255.255 y se encuentran reservadas para servicios de investigación.

En general, tanto en redes LAN como en WAN se utiliza el direccionamiento de clases A, B o C dependiendo de la cantidad de redes necesarias y la cantidad de computadoras (hosts) a cubrir. A continuación, se desarrollará más profundamente la división de clases de red esbozada anteriormente, y se explicará cómo varía la cantidad de redes y hosts que puede cubrir cada clase de IP.

### *Entienda los IP Addresses*

*Una dirección IP es un direccionamiento usado para identificar únicamente un dispositivo en una red del IP. El direccionamiento se compone de 32 bits binarios, que pueden ser divisibles en una porción de la red y recibir la porción con la ayuda de una máscara de subred. Los 32 bits binarios se dividen en cuatro octetos (1 octeto = 8 bits). Cada octeto se convierte a decimal y se separa con un punto. Por esta razón, se dice que una dirección IP se expresa en formato decimal con puntos (por ejemplo, 172.16.81.100). El valor en cada octeto posee un rango decimal de 0 a 255 o binario de 00000000 a 11111111.*

*He aquí cómo se convierten los octetos binarios a decimal: La derecha la mayoría del bit, o bit menos significativo, de un octeto lleva a cabo un valor de $2^0$. El bit apenas a la izquierda de ése lleva a cabo un valor de $2^1$. Esto continúa hasta el bit más a la izquierda, o el bit más significativo, que lleva a cabo un valor de $2^7$. Por lo tanto, si todos los bits son un uno, el equivalente decimal sería 255 como se muestra aquí:*

```
  1  1  1  1 1 1 1 1
128 64 32 16 8 4 2 1 (128+64+32+16+8+4+2+1=255)
```

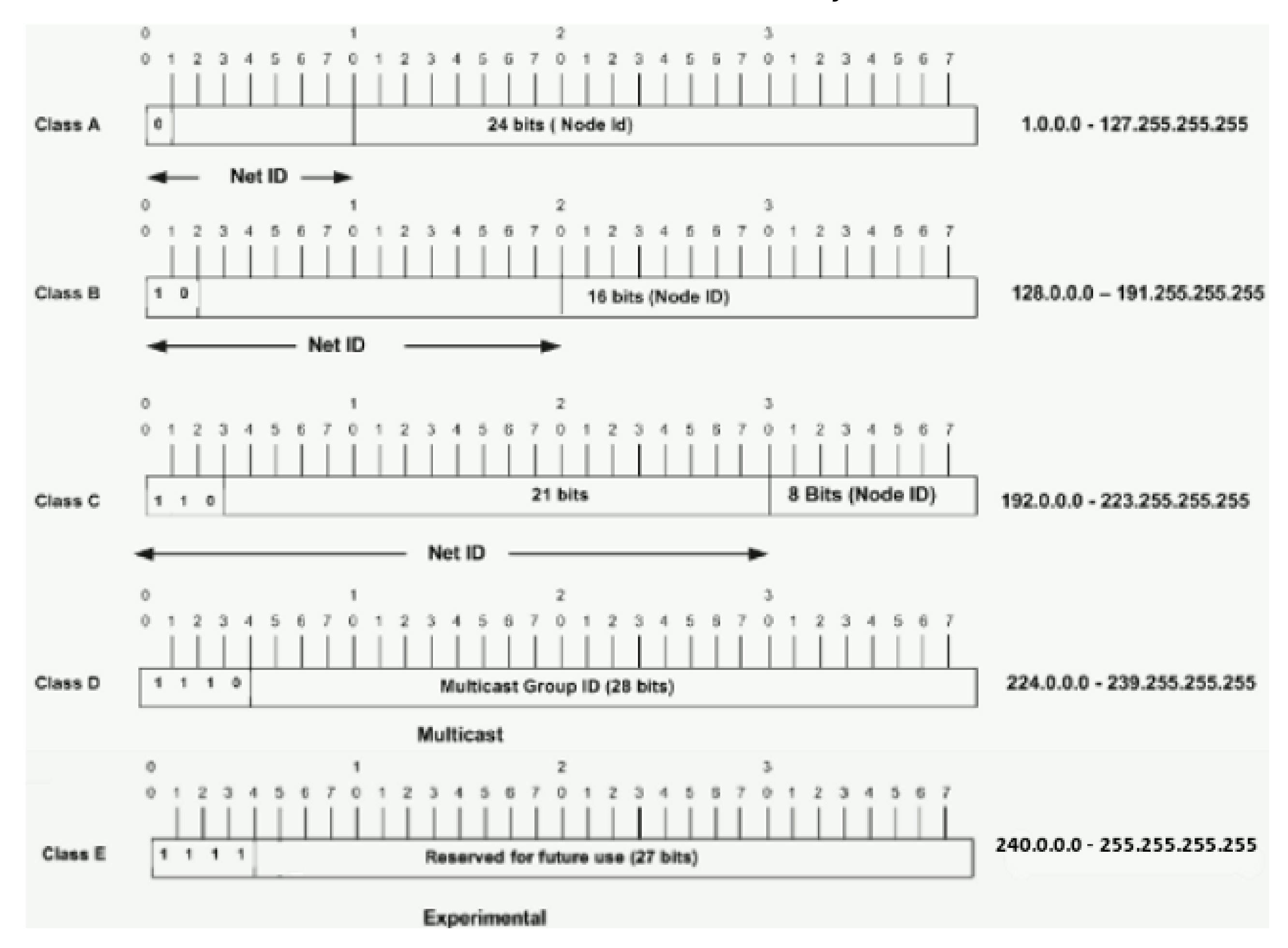
*He aquí una conversión de octeto de ejemplo cuando no todos los bits están establecidos en 1.*

```
0  1 0 0 0 0 0 1
0 64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)
```

*Y esta muestra muestra una dirección IP representada en el binario y el decimal.*

```
      10.      1.      23.      19 (decimal)
00001010.00000001.00010111.00010011 (binary)
```

*Dado un IP Address, su clase se puede determinar de los tres bits de orden alto (los tres bits más a la izquierda en el primer octeto). La Figura 1 muestra la significación de los tres bits de orden superior y el rango de direcciones que caen en cada clase. Para propósitos informativos, también se muestran direcciones de Clase D y Clase E.*




*Información e imagen obtenida de Documentación CISCO*

## Cálculo de clases IP

De la imagen anterior podemos encontrar un dato bien interesante, las direcciones de red (identificadas como "Net ID") comprenden dependiendo de la clase, una cantidad de bits diferentes:

- **En la clase A:** La dirección de red sólo está compuesta por 8bits, mientras que los otros 24 bits son utilizables para que el administrador de redes divida los hosts según considere conveniente, entonces el primer octeto corresponde a las direcciones de red diferentes, quedando **sólo el primer bit fijo dentro del rango de las redes clase A**. Esto es:
  - ➢ Expresadas en binario, las direcciones de clase A van desde la **0**0000000.00000000.00000000.00000000 hasta la **0**1111111.11111111.11111111.11111111. Por eso las direcciones de clase A van desde la 0.0.0.0 hasta la 127.255.255.255 (Aquí y en los ejemplos

siguientes, marcamos en rojo las direcciones de red y en verde las de host, marcando en **negrita** los bits que son característicos de las direcciones de la clase)

- ➢ Esto implica que las redes de clase A deben comenzar necesariamente con un 0 en su primer octeto, seguido de 7 bits, y así dependiendo del valor pueden comprender desde el 0 hasta la 127, teniendo posibles hasta 128 redes diferentes. Cada red, puede atender a su vez hasta a 256*256*256 (-2 por direcciones de puerta de red y difusión) = 16.777.214 hosts.

- **En la clase B,** las direcciones de red están comprendidas por tanto el primero y el segundo octeto de la cadena, es decir, tenemos 16 bits de direcciones de red y 16 bits para direcciones de host. Las direcciones de red comenzarán a partir de la siguiente a la última dirección de red de clase A, es decir, a partir de la 128, y en lugar de 1, tendremos los **dos primeros bits** de la secuencia como característicos de las IP de clase B. A continuación desarrollamos esto más claramente en binario y explicamos, como siempre, en rojo los bits de red, y en verde los de host:
  - ➢ Expresándolo en binario, las direcciones de clase B van desde la **10**000000.00000000.00000000.00000000 hasta la **10**111111.11111111.11111111.11111111, por eso su equivalencia decimal desde la 128.0.0.0 hasta 191.255.255.255.
  - ➢ Esto implica que en la clase B puede haber hasta (191-127)*256 = 16384 redes diferentes y hasta 256*256 (-2 por direcciones de red y difusión)= 65.534 hosts atendidos para cada red.

- **En la clase C**, las direcciones de red están comprendidas por el primero, el segundo y el tercer octeto de la cadena, es decir, que tenemos 24 bits en direcciones de red y 8 bits para direcciones de hosts. Las direcciones de red comenzarán a partir de la siguiente a la última dirección de red de clase B, y tendremos **los tres primeros bits** de la secuencia fijos para las IP de clase C. Esto es:
  - ➢ Expresándolo en binario, las direcciones de clase C van desde la **110**00000.00000000.00000000.00000000 hasta la **110**11111.11111111.11111111.11111111, por eso su equivalencia decimal desde la 192.0.0.0 hasta 223.255.255.255.
  - ➢ Esto implica que en la clase C podemos tener hasta (223-191)*256*256 = 2.097.152 redes diferentes y hasta 256 (-2 por direcciones de red y difusión) = 254 hosts para cada red.

### *Máscaras de red*

*Una máscara de red ayuda a saber qué parte de la dirección identifica la red y qué parte de la dirección identifica el nodo. Las redes de la clase A, B, y C tienen máscaras predeterminadas, también conocidas como máscaras naturales, como se muestra aquí:*

*Class A: 255.0.0.0*

*Class B: 255.255.0.0*

*Class C: 255.255.255.0*

*Una dirección IP de una red de la Clase A que no se haya convertido en subred tendrá un par dirección/máscara similar a: 8.20.15.1 255.0.0.0. Para ver cómo la máscara le ayuda a identificar a las partes de la red y del nodo el direccionamiento, convierta el direccionamiento y la máscara a los números binarios.*

*8.20.15.1 = 00001000.00010100.00001111.00000001*

*255.0.0.0 = 11111111.00000000.00000000.00000000*

*Una vez que usted hace el direccionamiento y la máscara representar en el binario, después la identificación de la red y del ID del host es más fácil. Cualquier bit de dirección que tenga el bit de máscara correspondiente establecido en 1 representa la identificación de red. Cualquier bit de dirección que tenga el bit de máscara correspondiente establecido en 0 representa la identificación de nodo.*

*8.20.15.1 = 00001000.00010100.00001111.00000001*

*255.0.0.0 = 11111111.00000000.00000000.00000000*

-----------------------------------

*net id* | *host id*

*netid = 00001000 = 8*

*hostid = 00010100.00001111.00000001 = 20.15.1*

(Documentación CISCO)

## Cálculo de IP dependiendo de requerimientos y Subnetting

Antes de seguir adelante desarrollando este tema, debemos tener bien claras algunas definiciones muy breves correspondientes a este tema:

- ***Direccionamiento -*** *El número único ID asignado a una host o interfaz en una red.*
- ***Subred -*** *Una porción de una red que comparte a una dirección de subred determinada.*
- ***Máscara de subred -*** *Una combinación de 32 bits usada para describir que la porción de un direccionamiento refiere a la subred y que refiere la parte al host.*
- ***Interfaz -*** *Una conexión de red.*

(Documentación CISCO)

Anteriormente ya se trabajó sobre las diferentes clases de direcciones IP, con el concepto de máscara y que éstas direcciones en diferentes clases permiten diferentes cantidades de equipos o de redes dependiendo de la clase.

A su vez, es necesario aclarar que se puede calcular cuántas redes podemos obtener a partir de una dirección IP con su respectiva máscara, y cuántas terminales puede soportar, todo eso con unos pequeños cálculos, simplemente teniendo claro cómo trabajar en binario y manejando potencias en base 2, vamos a ello:

### *Subnetting*

Resulta poco realista suponer que sólo se pueden utilizar redes de clase A, B, C, D o E, siendo que la cantidad de posibilidades que ofrecen las clases de IP resulta limitada, podemos extender por mucho la cantidad de redes y equipos a conectar, creando divisiones lógicas en redes de cualquier clase, mediante lo que se conoce como **subredes**.

Para esto, a partir de una dirección IP y una máscara de subred, podemos extender la máscara (agregarle bits significativos, es decir, 1s a la izquierda) y agrandando así la dirección de red , para crear mayor cantidad de redes (subredes) con una cantidad más pequeña de hosts en cada una.

**Explicación:**

- Tenemos por ejemplo una red cuya IP es 223.176.10.0 con una máscara de subred 255.255.255.0. **En este caso de ejemplo, es una red de clase C,** pero para lo que vamos a hacer, esto nos es indiferente, simplemente crearemos subredes de clase C, este esquema nos indica que en esta red, tenemos un 0 en el último octeto de la máscara de subred, es decir que podría abastecer hasta **254** equipos.
    - Sabemos esto porque en el último octeto de la máscara hay un 0, lo que quiere decir que tenemos 8 bits posibles para direccionar terminales o nodos, lo que se traduce en 256 posibilidades – 2 que están reservadas para la primera dirección (Red) y la última (Broadcast).
    - El razonamiento anterior también responde a una operación sencilla, 2 elevado a la cantidad de bits en 0 disponibles en la máscara sería $2^8$ = 256, quitándole 2 por las direcciones de Subred y Broadcast nos resulta en 254 nodos.
- Podemos crear a partir de la máscara dada más cantidad de subredes, con menor cantidad de nodos en cada una, cuanto más 1s le agreguemos a la máscara, más cantidad de subredes podremos cubrir pero nos quedarán menor cantidad de 0s, pudiendo abarcar menor cantidad de hosts. Digamos que si le agregamos $2^n$ cantidad de 1s, podremos sacar hasta $2^n$ cantidad de subredes, pero la cantidad de hosts a abarcar será con la misma lógica dependiendo de la cantidad de 0s.
- Vamos a agregar para este caso 3 1s al principio del último octeto de la máscara, con lo cual, la máscara natural que era:

11111111.11111111.11111111.00000000, nos queda en:
11111111.11111111.11111111.**111**00000.
En notación decimal, la máscara extendida resultante nos quedó en 255.255.255.**224,** teniendo como resultado una nueva división donde podremos crear $2^3$ cantidad de subredes, es decir, hasta 8 subredes diferentes.

- La cantidad de hosts que podremos abarcar en cada subred con la nueva máscara especificada será 2 elevado a la cantidad de 0s que dejamos en la máscara

(menos 2), en este caso 5, y tenemos $2^5 = 32$, menos las IPs de Subred y Broadcast tenemos hasta 30 equipos para cada subred.

- Como resultado, tenemos que con la misma IP original de red 223.176.10.0, extendiendo la máscara a 255.255.255.224 obtenemos las siguientes subredes:

| Nº de subred | Dirección de subred | Dirección de broadcast |
|---|---|---|
| 0 | 223.176.10.0 | 223.176.10.31 |
| 1 | 223.176.10.32 | 223.176.10.63 |
| 2 | 223.176.10.64 | 223.176.10.95 |
| 3 | 223.176.10.96 | 223.176.10.127 |
| 4 | 223.176.10.128 | 223.176.10.159 |
| 5 | 223.176.10.160 | 223.176.10.191 |
| 6 | 223.176.10.192 | 223.176.10.223 |
| 7 | 223.176.10.224 | 223.176.10.255 |

- **Los equipos comprendidos en la subred 1, tomarán las IPs comprendidas entre la 223.176.10.1 y la 223.176.10.30, los comprendidos en la subred 2 tomarán las IPs que van desde la 223.176.10.33 hasta la 223.176.10.62 y así sucesivamente.**
- **A partir de la primera dirección de subred, las siguientes comenzarán tomarán direcciones en una cantidad igual a 256 / (cantidad de subredes), en este caso, 256/8 = 32 direcciones. (Ej:223.176.10.0, 223.176.10.32, 223.176.10.64, etc)**

### *Cálculo de subredes dependiendo de los requerimientos:*

La cantidad de subredes que podemos crear a partir de una dirección IP y su máscara va a depender directamente de la cantidad de 0s disponibles en la máscara de subred (expresada en binario), al mismo tiempo, a mayor cantidad de subredes creadas, menor cantidad de hosts para cada subred, en el ejemplo anterior tenemos una red de clase C dividida en 8 subredes con hasta 30 hosts cada una. En el caso de tener 4 subredes podríamos tener hasta 62 hosts por cada subred, ya que en lugar de 3 bits en 1, habríamos agregado 2, y nos quedarían 6 bits en la máscara con 0s para dirigir hosts ($2^6 = 64$ -2 de dirección de red y difusión de cada subred).

De forma genérica, para crear subredes tendremos que extender la máscara, agregando 1s en los bits que tiene disponibles en 0, y nos encontramos con el siguiente esquema:

- **Si n es la cantidad de 1s que le agregamos a la máscara, $2^n$ va a ser la cantidad de subredes que vamos a poder abarcar.**
- **Si h es la cantidad de 0s que le dejamos a la máscara ampliada, $2^h-2$ va a ser la cantidad de equipos que va a poder alcanzar cada subred.**

***Entonces, ¿Cuántas subredes y hosts puedo obtener a partir de una máscara de subred?***

- Todo va a depender de la cantidad de 0s disponibles en la máscara, si la máscara de subred es de la forma: 255.255.0.0 (máscara de clase B) tenemos enteros los dos últimos octetos en 0, lo cual quiere decir que en binario tenemos 16 bits en 0 que podemos subdividir y repartir para crear subredes y hosts según sea necesario.
- Si la máscara es de la forma 255.255.255.0 (máscara de clase C) tenemos libre todo el último octeto, es decir, 8 bits para poder hacer dicha repartición.
- Una vez que identificamos la cantidad de 0s disponibles en la máscara, procedemos a retomar la regla anterior, y agregamos 1s según corresponda.

## *Ejercicios de ejemplo con subredes de clase C*

a. **Si tengo la IP 192.168.2.0 con la máscara 255.255.255.0, crear subredes para poder abarcar al menos 90 equipos en cada una.**

- Para este caso, ya sabemos que la máscara tiene un 0 decimal en el último octeto, es decir, 8bits en 0 de los cuales podemos crear la subdivisiones según convenga.
- Necesitamos abastecer 90 equipos por subred, así que tenemos que buscar un número **h** de cantidad de 0s a dejar en la máscara que sea mayor o igual a 92 (recordar siempre que 2 direcciones quedan reservadas para dirección de red y broadcast, y 90+2 = 92); dicho número **h** debe ser tal que $2^h \geq 92$, y ese número es 7, ya que 2 elevado a la séptima potencia nos da 128, que es mayor a 92. Podríamos intentar reducir este número, pero con h=6 no nos alcanzaría para todos esos hosts, teniendo en cuenta que $2^6 = 64$.
- Para abastecer al menos 90 equipos, sabemos que debemos dejar 7 bits en la máscara en 0, y teníamos originalmente 8 bits en 0, con lo cual sólo podemos agregar un 1 significativo. La máscara expresada en binario pasaría de ser 11111111.11111111.11111111.**0**0000000 a ser 11111111.11111111.11111111.**1**0000000, es decir que la nueva máscara extendida nos quedará en 255.255.255.128 (128 porque “10000000” en binario es equivalente a ese valor decimal) y como cambiamos sólo 1 bit de red, entonces podremos obtener hasta $2^1$ cantidad de subredes, o lo que es lo mismo, 2 subredes.
- El esquema resultante nos deja con 2 subredes, dispuestas del siguiente modo:

| Subred | Dirección de red | Dirección de broadcast |
|---|---|---|
| 0 | 192.168.2.0 | 192.168.2.127 |
| 1 | 192.168.2.128 | 192.168.2.255 |

- Nótese que entre subredes el número avanza 128 lugares, ya que 256 / (cantidad de subredes), es decir 256/2 = 128.
- Las direcciones de los equipos en la primera subred irán desde la 192.168.2.1 hasta la 192.168.2.126 y en la segunda subred (la 1) desde la IP 192.168.2.129 hasta la 192.168.2.254

b. **Para la red 192.168.10.0 con mascara 255.255.255.0, obtener 8 subredes**.

- En primer lugar aquí, debemos saber si podemos crear 8 subredes con la máscara ofrecida, siendo que la máscara tiene en 0 todo el último octeto (8 bits en 0) tenemos que agregar **1**s en la máscara, en una cantidad **n,** de tal modo que **$2^n$ sea igual a 8.** La cantidad de 1s a agregar entonces será 3, porque **$2^3$ = 8.**
- Como debemos agregar 3 bits en 1 a la máscara para poder crear las 8 subredes, y tenemos 8 bits en 0 (está libre todo el último octeto), entonces podemos crear nuestra nueva máscara extendida, donde la máscara original que era (en binario) 11111111.11111111.1111111.**000**00000 pasará a ser 11111111.11111111.1111111.**111**00000. es decir que la nueva máscara extendida será **255.255.255.224** y como resultado tendremos un número **h** de bits en 0 igual a 5, es decir que podremos conectar **$2^5$ - 2 = 30** equipos en cada subred.
- Con la nueva máscara 255.255.255.224 tenemos las siguientes subredes como resultado:

| Subred | Dirección de subred | Dirección de broadcast |
|---|---|---|
| 0 | 192.168.10.0 | 192.168.10.31 |
| 1 | 192.168.10.32 | 192.168.10.63 |
| 2 | 192.168.10.64 | 192.168.10.95 |
| 3 | 192.168.10.96 | 192.168.10.127 |
| 4 | 192.168.10.128 | 192.168.10.159 |
| 5 | 192.168.10.160 | 192.168.10.191 |
| 6 | 192.168.10.192 | 192.168.10.223 |
| 7 | 192.168.10.224 | 192.168.10.255 |

**Los equipos comprendidos en la subred 1, tomarán las IPs comprendidas entre la 192.168.10.1 y la 192.168.10.30, los comprendidos en la subred 2 tomarán las IPs que van desde la 192.168.10.33 hasta la 192.168.10.62 y así sucesivamente.**

**c. Si tengo la dirección de red 192.168.2.0 con una máscara 255.255.255.0, ¿Puedo obtener 4 subredes con 80 hosts cada una?**

- Como en todos los ejercicios de cálculo de subredes, el primer paso es comprobar si se pueden tener esas subredes con la configuración especificada. Como la

máscara termina en 0, quiere decir que los 8 bits del último octeto son 0s, y para obtener 4 subredes necesitamos agregar a la máscara **una cantidad n de bits en 1 tal que $2^n = 4$**, como ya nos pasó antes, ese número es 2, ya que $2^2 = 4$.

- Sin embargo, agregando 2 bits en 1 a la máscara de subred especificada, nos quedarían 6 bits en 0 disponibles para equipos, limitando la cantidad de equipos a **$2^6 - 2 = 62$ estaciones para cada subred.**
- Como conclusión para este ejercicio, podremos deducir que no es posible tener con la configuración especificada 4 subredes con 80 hosts, sino que tendríamos como máximo 62 hosts para cada subred (si dividimos en 4 subredes).

## Máscaras de subred con notación barra diagonal

De los ejercicios anteriores se deducen varias cosas: Una de ellas es que el cálculo de subredes no es complicado, pero sí que tenemos que prestar atención en las operaciones; la segunda, es que es bastante engorroso trabajar todo el tiempo con la dirección IP de una red y la máscara de subred con la notación tradicional (Ej: 255.255.255.0) para después pasar esa máscara de subred a binario a la hora de trabajar.

Siendo que a la hora de hacer Subnetting, los cálculos los hacemos en base a los bits de la máscara de subred, y las operaciones las hacemos en binario, existe una notación más fácil para representar la máscara de subred de cualquier equipo, y es con la barra diagonal. Nos resultará mucho más fácil calcular la cantidad de host y de subredes que podemos obtener con esta nueva notación.

Para ello simplemente se coloca la dirección IP separada de una barra con la cantidad de 1s que posee la máscara de subred, ejemplo:

192.198.10.0/**24** quiere decir que tenemos 24 1s en la máscara de subred, es decir, que la máscara tiene la forma:

**11111111.11111111.11111111**.00000000

O lo que es lo mismo, que la máscara es 255.255.255.0 lo que refiere a una red de clase C.

<u>Ejemplo:</u>

- La red con dirección 192.168.55.0/29 implica que tenemos 29 1s en la máscara de subred, o lo que es lo mismo, quiere decir que la máscara de subred es: **11111111.11111111.11111111.11111**000 lo que implica directamente que estamos trabajando con una **<u>subred de clase C</u>**, con 5 bits en el último octeto en 1, y 3 bits en 0.
- Las subredes de clase c tienen por defecto 24 bits en 1, lo que quiere decir que tiene 29-24 = 5 bits prestados en su máscara extendida, lo que directamente nos indica que es una red dividida en **$2^5 = 32$** subredes con hasta **$2^3-2 = 6$** hosts en cada subred (recordar siempre que restamos 2 hosts por las direcciones de red y broadcast)

## Obteniendo direcciones de subred o de host de manera directa

Supongamos que ya hemos creado subredes a partir de una red dada, y necesitamos saber la dirección de una subred o un equipo en específico, existe una manera muy sencilla de hacerlo sin tener que recurrir a la tabla que armamos con cada respectiva subred, lo cual sería muy necesario sobre todo en redes donde tenemos cientos o miles de subredes.

- En primer lugar debemos obtener el número binario equivalente al número de la subred que queremos obtener. **Debe ser expresado en la misma cantidad de bits como los que hayamos cambiado en la máscara extendida.**
- Pasamos a binario toda la secuencia de red y en los bits más significativos (más a la izquierda) de las direcciones de host colocamos el binario correspondiente al número de subred que queremos obtener.
- Obtenemos el decimal correspondiente y entonces tendremos la dirección de red de la subred correspondiente.
- Una vez que tenemos la dirección de la subred, será mucho más fácil obtener el número del equipo correspondiente, ya que bastaría con sumarle al número de la subred, el número del host del cual queremos obtener su IP (para subredes de clase C).

Ejemplo:

Para explicar este mecanismo, consideremos una división existente de un ejemplo anterior, como ser la IP **192.168.10.0** con la máscara extendida **255.255.255.224**, la tabla correspondiente era la siguiente:

| Subred | Dirección de subred | Dirección de broadcast |
|---|---|---|
| 0 | 192.168.10.0 | 192.168.10.31 |
| 1 | 192.168.10.32 | 192.168.10.63 |
| 2 | 192.168.10.64 | 192.168.10.95 |
| 3 | 192.168.10.96 | 192.168.10.127 |
| 4 | 192.168.10.128 | 192.168.10.159 |
| 5 | 192.168.10.160 | 192.168.10.191 |
| 6 | 192.168.10.192 | 192.168.10.223 |
| 7 | 192.168.10.224 | 192.168.10.255 |

Supongamos que queremos obtener la dirección IP del 11º equipo de la subred número 5:

- 5 en binario es **101 (no tenemos que agregar 0s a la izquierda porque precisamente, cambiamos 3 bits en la máscara).**

- Pasando toda la cadena de la red a binario, tendríamos que la dirección de red (192.168.10.0) equivale a: 11000000.10101000.00001010.00000000
- Colocando el 101 a la izquierda de las cifras marcadas en verde, nos queda la siguiente IP resultante (en binario) que será la de nuestra subred, en este caso, de la subred Nº5: 11000000.10101000.00001010.**101**00000.
- Pasando a decimal dicha dirección, tenemos que la dirección de subred correspondiente a la quinta (sexta) subred creada, es la **192.168.10.160** lo que podemos comprobar que coincide con la tabla.
- Como queríamos obtener la dirección del host 11 de dicha subred, sumamos 160 + 11 = 171, por lo cual, la IP del equipo Nº11 de la subred Nº5 es 192.168.10.171.

Supongamos ahora, que queremos obtener la dirección IP Nº5 de la subred número 3:

- 3 en binario es **11, pero lo expresamos como 011 (agregamos un 0 a la izquierda para que quede con 3 bits que es lo que cambiamos en la máscara)**
- Pasando toda la cadena de la red a binario, tendríamos que la dirección de red (192.168.10.0) equivale a: 11000000.10101000.00001010.00000000
- Colocando un 011 a la izquierda de la dirección de host de la red, o lo que es lo mismo, en el espacio donde pasamos a extender la subred (indicado en verde) nos queda que la dirección IP de la subred 3 en binario es: 11000000.10101000.00001010.**011**00000, por lo que expresada en decimal, la dirección de subred de la cuarta subred (la número 3) es: **192.168.10.96**, lo que también coincide con la tabla que armamos.
- Ahora para obtener la IP del quinto equipo de la subred 3, simplemente sumamos 96+5 = 101 por lo que su IP es **192.168.10.101**

**Ahora confiando en el método anterior, estamos en condiciones de obtener cualquier IP de cualquier subred que exista, y con ella la dirección de cualquier número de equipo de dicha subred. Lo que será especialmente útil en esquemas cuya cantidad de subredes no sea práctico representar en una tabla para guiarnos.**

### *Ejercicios de subredes clase A y B*

**a. Obtener un mínimo de 100 subredes partiendo de la IP 10.0.0.0, máscara 255.0.0.0, obtener las direcciones de las subredes 22, 36, 45 y 78**

- Para este caso lo primero que debemos observar es la máscara de red, que tiene la forma 255.0.0.0, esto quiere decir que podemos tomar subredes de cualquier dirección a partir del segundo octeto que está completamente en 0. El primer octeto es tomado por completo por la dirección de la red, y los otros hasta el momento están disponibles para terminales, por lo cual deducimos que es una red de clase A.

- Si vamos a modificar el segundo octeto, tenemos 256 posibilidades para subredes, tomando direcciones entre el 0 y el 256, si ocupamos 7 bits para subredes, podremos abarcar **$2^7$= 128** subredes diferentes, si ocupamos 6 podremos abarcar apenas **$2^6$ = 64**, así que optamos por modificar los 7 primeros bits para subredes. Eso quiere decir que la nueva máscara extendida tomará en binario la forma:
- 11111111.**1111111**0.00000000.00000000 o su equivalente decimal será **255.254.0.0**
- La cantidad de equipos que podremos colocar en cada subred será tomando cualquiera de los bits en 0 de la subred extendida, es decir que podremos tener ($2^8$ * $2^8$ * $2^1$) – 2 = 131.070 hosts para cada subred.
- Las subredes resultantes serán entonces:

| **Nº de subred** | Dirección de subredred | Broadcast |
|---|---|---|
| 0 | 10.0.0.0 | 10.1.255.255 |
| 1 | 10.2.0.0 | 10.3.255.255 |
| ... | ... | ... |
| 127 | 10.254.0.0 | 10.255.255.255 |

**Obtener las direcciones de las subredes 22, 36, 45 y 78:**

- Primero que nada vamos a pasar a binario el número 22: Nos da **10110, pero lo expresamos como 0010110 porque hemos cambiado 7 bits de la máscara.**
- En segundo término, tomamos toda la dirección IP original en binario y colocamos el número de la subred que queremos obtener (0010110) en su segundo octeto:
- 00001010.**0010110**0.00000000.00000000
- Pasando a decimal la cadena anterior, obtenemos que la dirección de la subred Nº22 es: **10.44.0.0**

***Ahora que notamos que 44 es (22*2) ya que para este caso particular la dirección de subred (en decimal) es siempre par y va de a 2 en 2, para este caso particular, podemos deducir que:***

- La subred Nº36 tiene la forma 10.72.0.0
- La subred Nº45 tiene la forma 10.90.0.0
- La subred Nº78 tiene la forma 10.156.0.0

*A tener en cuenta:*

Recordar que las máscaras de red de la clase A son de la forma 255.0.0.0, en la clase B, 255.255.0.0 y en la clase C, 255.255.255.0. Al hacer subredes, podremos dividir la red en los lugares donde la máscara tiene representado un 0.

**b. A partir de la dirección 176.141.0.0/16 obtener subredes para al menos 2000 hosts en cada subred. Luego obtener la dirección de los equipos 130, 225 y 1604 de la cuarta subred.**

- Para este ejercicio lo primero que tenemos que tener en cuenta es que nos estamos enfrentando a una dirección IP de **clase B**, y lo sabemos por el primer octeto de la IP (176), que pertenece a dicha clase (recordemos que entre 128 y 191 pertenece a clase B).
- Además, sabemos que la **máscara es de una red de clase B**, ya que el "/16" nos indica que la máscara tiene 16 1s significativos, sería: 1111111.1111111.00000000.00000000
- La primera pregunta a resolver es, ¿Podemos obtener subredes de 2000 hosts c/u a partir de una red de clase B?. Sabemos que las redes de clase B pueden tener hasta $2^8 * 2^8 - 2$ hosts, es decir, 65.534 hosts, lo que es mucho más alto que 2000, de modo que sí, podemos obtener dichas subredes. La siguiente pregunta es, ¿Cuántos 0s debemos dejar como mínimo en la máscara extendida para soportar 2000 hosts?
- Probamos, si dejamos 10 0s tendremos $2^{10}$-2 posibles hosts, es decir, 1022. Con lo cual resulta insuficiente, si dejamos 11 0s tendremos $2^{11}$(-2 por direcciones de subred y broadcast) es decir, 2046 posibilidades.
- Tenemos que dejar 11 0s a la derecha de la máscara, lo cual nos permite agregar 5 1s a la dirección de red, para la subred extendida, la máscara de subred pasará a ser entonces 11111111.11111111.**11111**000.00000000. En su notación decimal, la nueva máscara extendida es **255.255.248.0** y nos permitirá crear subredes de clase B. Concretamente nos dejará tener hasta $2^5$ = 32 subredes diferentes con hasta 2022 terminaciones para cada subred de clase B.
- Como resultado, nos queda el siguiente esquema de subredes, partiendo de la IP 176.141.0.0:

| Nº de subred | Dirección de subred | Dirección de Broadcast |
|---|---|---|
| 0 | 176.141.0.0 | 176.141.7.255 |
| 1 | 176.141.8.0 | 176.141.15.255 |
| … | … | … |
| 31 | 176.141.248.0 | 176.141.255.255 |

- Notar que las direcciones de subredes cambian de a 8 direcciones en el tercer octeto, cambian en este octeto porque son subredes de clase B, y cambian de a 8 direcciones debido a que van de a 256 / (cantidad de subredes) es decir 256 / 32 = 8 direcciones.

**Luego obtener la dirección de los equipos 130, 225 y 1604 de la cuarta subred:**

Sabiendo que las subredes van de a 8 lugares en el segundo octeto, sacar la cuarta subred es muy fácil, la cuarta subred será la Nº3 (porque comienzan en 0) así que simplemente hacemos 8*3 = 24, sabemos que la cuarta subred es la que tiene dirección número **176.14.24.0**

Igualmente lo podemos hacer al método tradicional, convertimos el 3 en binario (11) le agregamos la cantidad de 0s a la izquierda **para que quede con la misma cantidad de bits de los que hemos cambiado en la máscara**, en este caso **5**, nos queda (**00011**).

La dirección de subred toda expresada en binario será entonces: 10110000.00001110. **00011**000.00000000 lo que en su notación decimal, es igual a **176.14.24.0**.

- La Dirección de host Nº130 es muy fácil de obtener, simplemente sumamos 130 a la dirección en el último octeto de la cuarta subred, nos queda **176.14.24.130.**
- Obtener el host Nº225 también es igual de sencillo, ya que sumamos 225 en el último octeto, y nos queda **176.14.24.225.**
- Obtener el host Nº1604 de la cuarta subred es un poco más complicado, ya que el 1604 es demasiado grande para caber en el último octeto, su valor binario es mayor a 8 bits, por lo cual obviamente su IP hace cambiar algún número en el tercer octeto de toda la cadena.
- 1604 en binario es 11001000100, es decir, tiene **11 bits**, y en el último octeto apenas tenemos 8 bits, así que para sacar su dirección simplemente agregamos ese número expresado en binario en la dirección de host de toda la cadena de la dirección de IP (en binario): 10110000.00001110. 00011110.01000100 con lo cual, sacamos su notación decimal: **176.14.30.68**

➢ **Importante:** Vemos entonces que otro modo de encontrar la dirección IP de un determinado host dentro de una subred, basta con convertir a binario el número de host que nos interesa, y agregarlo a continuación de la dirección IP de subred correspondiente (expresada en binario).

**Más ejercicios e información adicional:**

En esta guía se ha intentado explicar a través de ejemplos, la lógica del direccionamiento IP y de la creación de subredes. Si se desea obtener información más detallada se sugiere visitar cualquiera de las siguientes direcciones:

- Documentación CISCO
- Ejercicios de la web QUIA

## Protocolos ARP y RARP

Relacionado con el direccionamiento lógico de equipos y por ende con la capa de red, intervienen los protocolos ARP y RARP, que relacionan direcciones IP con direcciones de hardware.

### Protocolo de Resolución de Direcciones (ARP)

“Adress Resolution Protocol” en Inglés, Es un protocolo que permite encontrar la dirección de hardware (Dirección MAC en Ethernet) que corresponde a una dirección IP. Para ello se envía un paquete a la dirección de difusión de la red (broadcast) que pertenece a la máquina con la IP por la que se pregunta, y se espera a que esa máquina (u otra) responda con la dirección MAC que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección de hardware, pero esto **solo**

**funciona si todas las máquinas lo soportan.** El protocolo ARP permite a un dispositivo conectado a una red LAN **obtener la dirección MAC de otro dispositivo conectado a la misma red LAN cuya dirección IP es conocida**.

*ARP se utiliza en cuatro casos referentes a la comunicación entre dos hosts:*

1. *Cuando dos hosts están en la misma red y uno quiere enviar un paquete a otro.*
2. *Cuando dos hosts están sobre redes diferentes y deben usar un gateway o router para alcanzar otro host.*
3. *Cuando un router necesita enviar un paquete a un host a través de otro router.*
4. *Cuando un router necesita enviar un paquete a un host de la misma red.*

(Wikipedia)

**Protocolo de Resolución de Direcciones Reverso (RARP)**

El protocolo Reverse ARP utiliza el mismo mecanismo que ARP, pero a partir de una dirección de hardware (Ethernet MAC) permite obtener la dirección IP de una estación. Dicha dirección debe pertenecer a un equipo conectado a la misma red local. Además de ser útil en redes Ethernet, también sirve para otras redes de área local, como ser por ejemplo la Interfaz de Fibra de Distribución de Datos o las LAN Token Ring.

Para poderse utilizar RARP todas las direcciones MAC debían estar configuradas en un servidor central que pudiera transferir una dirección IP, no obstante, RARP ya ha quedado en desuso, primero fue sustituido por BOOTP y posteriormente por el Protocolo de Configuración Dinámica de Host (DHCP).

### *Probando el protocolo ARP*

El funcionamiento del protocolo ARP podemos probarlo desde nuestra computadora si se encuentra conectada a una LAN, desde la consola de comandos.

- A nivel básico, podemos tipear *arp –a* que nos mostrará todo el caché actual de las tablas ARP de todas las interfaces de red conectadas a nuestra misma red. Si queremos obtener la dirección de hardware debemos agregar a este comando la dirección IP de destino, ejemplo *arp –a 192.168.2.7*
- Si tipeamos *arp /?* El sistema nos mostrará la ayuda de la línea de comandos para esta orden.
- Probaremos entonces, ingresar el comando *arp –a* para ver qué resultado produce en el equipo en el cual se escribe actualmente, conectado a una red LAN, y a su vez, conectado a Internet:

```
C:\Users\vicmn>arp -a

Interfaz: 192.168.5.7 --- 0x14
  Dirección de Internet          Dirección física      Tipo
  192.168.5.1           a0-f3-c1-01-2c-32     dinámico
  192.168.5.63          ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático

C:\Users\vicmn>_
```

## Servicio DHCP

Anteriormente ya se ha trabajado con el protocolo IP como el más importante en capa de red ya que se encarga del direccionamiento lógico de equipos, trabajamos con las direcciones IP estáticas y dinámicas, y aclaramos que las direcciones dinámicas son aquellas que un servidor asigna a un equipo una vez conectado pero cuando dicho equipo se desconecta, al volver a conectarse a la red tendría otra IP diferente asignada por el servidor. A veces esto ocurre luego de pasado un período de tiempo, pero en cualquier caso la interfaz de red se configura a nivel lógico con la información proveída por un servidor. Esto se logra gracias al protocolo DHCP, el cual hemos mencionado antes pero aún no se había desarrollado,.

La sigla **DHCP** en español significa “Protocolo de Configuración Dinámica del Host”, es un protocolo de administración de red donde un servidor, asigna de forma automática los parámetros de configuración e red (tales como IP, máscara, puerta de enlace predeterminada y dirección de difusión) a los equipos terminales conectados a su red. Esto evita que cada vez que se conecta un equipo a la red, deba existir un administrador de red que configure manualmente cada equipo para que pueda comunicarse con el resto, es un servicio ampliamente utilizado en Internet por las compañías proveedoras de servicio (ISP). Este servicio, se puede utilizar en redes de variado tamaño, desde redes domésticas hasta redes de área de campus y aún más grandes, como ser en redes de regiones enteras donde existen servidores que proveen de Internet a un gran número de equipos.

Este servicio no obstante, puede ser implementado por un servidor, por una puerta de enlace residencial que actúe como servidor, o por un enrutador que tenga instalado dicho servicio. En breves veremos cómo se configura un servidor DHCP en un router CISCO (Se invita al lector a probar los comandos con Packet Tracer). Sin embargo, antes de esto, consideremos detallar algunas características:

*“Con DHCP, cada red debe tener un servidor DHCP responsable de la configuración. Al iniciar una computadora, ésta tiene integrada una dirección Ethernet u otro tipo de dirección de capa de enlace de datos en la NIC, pero no cuenta con una dirección IP. En forma muy parecida al ARP, la computadora difunde una solicitud de una dirección IP en*

*su red. Para ello usa un paquete llamado DHCP DISCOVER. Este paquete debe llegar al servidor DHCP. Si el servidor no está conectado directamente a la red, el enrutador se configurará para recibir difusiones DHCP y transmitirlas al servidor DHCP en donde quiera que se encuentre. Cuando el servidor recibe la solicitud, asigna una dirección IP libre y la envía al host en un paquete DHCP OFFER (que también se puede transmitir por medio del enrutador). Para que esto pueda funcionar incluso cuando los hosts no tienen direcciones IP, el servidor identifica a un host mediante su dirección Ethernet (la cual se transporta en el paquete DHCP DISCOVER). Un problema que surge con la asignación automática de direcciones IP de una reserva es determinar qué tanto tiempo se debe asignar una dirección IP. Si un host sale de la red y no devuelve su dirección IP al servidor DHCP, esa dirección se perderá en forma permanente. Después de un tiempo, tal vez se pierdan muchas direcciones. Para evitar que eso ocurra, la asignación de direcciones IP puede ser por un periodo fijo de tiempo, una técnica conocida como arrendamiento. Justo antes de que expire el arrendamiento, el host debe pedir una renovación al DHCP. Si no puede hacer una solicitud o si ésta se rechaza, tal vez el host ya no pueda usar la dirección IP que recibió antes"* (Tanembaum, 2014)

## Configurando un servidor DHCP

Supongamos que tenemos una red local y queremos que, en lugar de asignar manualmente la configuración de red a nuestros equipos, tengamos un servidor DHCP que lo haga por nosotros, y que conectar el equipo en red sea una tarea tan sencilla como conectar un cable del equipo al conmutador, o si tenemos Wi-Fi, simplemente conectándonos a la red correspondiente seleccionando su SSID.

Para ello, tenemos que tener el servicio DHCP funcionando en nuestra red, si tenemos un modem/router previamente instalado por nuestra ISP, seguramente ya tengamos el servicio DHCP corriendo en él, y configurado para ello, sin embargo, veamos cómo podemos realizar manualmente la configuración independientemente de nuestra compañía, realizando nosotros mismos la configuración.

Ante todo debemos tener en cuenta que, necesitamos un equipo que precisamente actúe como servidor DHCP, esto puede ser un router o una computadora utilizada como servidor, los pasos a seguir varían dependiendo del equipo y del sistema operativo, no obstante, como caso de estudio veremos cómo configurar el servicio DHCP en un router CISCO que actúe como servidor, y por otro lado en una computadora con Linux (Ubuntu) que funcionará como servidor del servicio. Cabe señalar, que existen routers que podemos adquirir a bajo costo en el mercado que permiten configurar el servicio DHCP sin entrar a escribir comandos como se describirá a continuación, simplemente siguiendo instrucciones por pantalla, pero para un mejor entendimiento del tema en cuestión, lo veremos “al modo difícil”. ¡manos a la obra!

### *Configurar servicio DHCP en router CISCO*

Para configurar DHCP en un enrutador CISCO, debemos conectarnos a él por medio de consola, como se ha explicado anteriormente en Configuración inicial por consola (utilizando el cable de consola y un emulador de terminal en nuestra PC, configurado para conectarse al dispositivo correspondiente), luego, debemos introducir en la terminal una serie de comandos:

A continuación tenemos el procedimiento:

- Primero debemos entra al modo de configuración Privilegiado con el comando "enable"

```
router>enable
```

- Entramos a el modo de configuración global "configure terminal"

```
router#configure terminal
```

- Creamos el pool de direcciones IP, esto es, darle un nombre al ámbito de direccionamiento, con el comando "ip dhcp pool [NOMBRE]"

```
router(config)#ip dhcp pool DHCP_1
```

- Indicamos el nombre de dominio con el commando "domain-name [DOMINIO]" Notar que en la línea del prompt se aprecia que nos hemos movido dentro de las aplicaciones del router, ya que ahora no nos muestra (config) sino (dhcp-config)

```
router(dhcp-config)#domain-name nombreelegido.com
```

- Especificamos el rango de direcciones IP a asignar en nuestro pool de direcciones, para ello usamos el comando "network [IP] [mascara], en este caso, vamos a asignar la dirección de red con máscara /24

```
router(dhcp-config)#network 192.168.10.0 255.255.255.0
```

- Especifica el tiempo máximo que puede asignarse una dirección IP a un nodo de la red. En este caso, el tiempo especificado es 1 días. Después de las 24 horas, el nodo hará un "Refresh" y se le asignará una nueva dirección IP.

```
router(dhcp-config)#lease 1
```

- Especifica los servidores de nombres de dominio (DNS).

```
router (dhcp-config)#dns-server 8.8.8.8 196.3.81.5
```

- Especifica la dirección de la puerta de enlace en la red LAN con el comando "default-router".

```
router(dhcp-config)#default-router 192.168.10.1
```

- Al final, salimos del modo configuración DHCP y podemos desconectar la terminal

```
router(dhcp-config)#exit
```

Si no hemos cometido errores sintácticos y el dispositivo ha aceptado todos los mensajes sin mostrar errores, entonces ya deberíamos tener el servicio DHCP activo en nuestra red, deberíamos practicarlo configurando cada equipo conectado para que obtenga la dirección IP de manera automática o dinámica, y luego de conectarlo a la red, observar qué dirección IP está adquiriendo.

### *Configurando DHCP utilizando un servidor Linux (Ubuntu)*

Supongamos que en lugar de tener un router CISCO tenemos una computadora con Linux que deseamos que funcione como servidor DHCP, para ello, aclaramos que esta configuración que trataremos es utilizando Ubuntu, ya que en otras distribuciones los comandos pueden variar un poco, así como la localización de los archivos que debemos configurar.

Configuración del servidor DHCP

- Primero debemos abrir un terminal e instalar el paquete DHCP del servidor, comando:

```
sudo apt-get install isc-dhcp-server
```

(Nota: Antes de Ubuntu 12.04 el paquete se llamaba dhcp3-server)

- Luego tendremos que cambiar la configuración predeterminada editando */etc/dhcp3/dhcpd.conf* para adaptarlo a sus necesidades y configuración particular. Para eso accedemos a modificar el archivo correspondiente con un editor de texto cualquiera, por ejemplo “nano”:

```
nano -w /etc/dhcp/dhcpd.conf
```

A dicho archivo debemos configurarlo con los parámetros que queramos asignarle a nuestro servidor DHCP, por ejemplo:

```
   ######### dhcpd.conf #########
#
option domain-name "nombrededominio.com";
option domain-name-servers dominio.ejemplo.com;
#

default-lease-time 7200;
max-lease-time 32400;
#
authoritative;
ddns-update-style none;
#
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.2 192.168.1.253;
  option routers 192.168.1.1;
  option broadcast-address 192.168.1.255;
  option netbios-name-servers 192.168.1.1;
```

```
}
#
#EOF
```

- ➢ Para este caso, estamos configurando como nombre de dominio “nombrededominio.com”, con un tiempo de espera predeterminado para que dure cada asignación de IP (tiempo de arrendamiento predeterminado) de 7200 segundos (2 horas), y con un tiempo máximo de arrendamiento de 32400 segundos (9 horas). Tenemos en este caso una dirección de la subred en 192.168.1.0/24, donde los equipos tomarán direcciones entre la 192.168.1.2 y la 192.168.1.253, dejando la 192.168.1.1 para el servidor y la 192.168.1.255 para la dirección de difusión. Se sugiere cambiar estos parámetros según conveniencia.
- ➢ La directiva “netbios-name-servers” colocada al final del archivo es opcional, se necesita setear en caso de que en nuestra subred tengamos también máquinas Windows, que requieran recibir direccionamiento desde nuestro servidor.

- También necesita editar */ etc / default / isc-dhcp-server* para especificar las interfaces que dhcpd debería escuchar. Por defecto escucha eth0 (debemos modificar este parámetro dependiendo de cuál sea la interfaz a usar como servidor).

```
nano -w /etc/default/isc-dhcp-server
```

Dentro del archio isc-dhcp-server colocamos la interfaz o interfaces que el servidor debería escuchar:

```
INTERFACES = "eth0"
```

- Además, debe asignar una dirección IP estática a la interfaz que usará para dhcp. Si va a usar eth0 para proporcionar direcciones en la subred 192.168.1.x, debe asignar, por ejemplo, ip 192.168.1.1 a la interfaz eth0 mediante la aplicación NetworkManager (se sugiere instalar) . Sin este paso, recibirá un error de dhcpd al iniciar el servicio.
- Por último, guardamos y reiniciamos el servidor DHCP (dhcpd)

```
sudo /etc/init.d/isc-dhcp-server restart
```

Cabe resaltar, que el servidor DHCP es un programa que puede reiniciarse, iniciarse o detenerse, sus respectivos comandos son:

- ➢ `sudo service isc-dhcp-server restart`
- ➢ `sudo service isc-dhcp-server start`
- ➢ `sudo service isc-dhcp-server stop`

- IMPORTANTE: Si necesitamos configurar las interfaces de red a mano (por jemplo para fijar una interfaz con una IP), podemos editar el archivo /etc/network/interfaces :

```
nano -w /etc/network/interfaces
```

Un ejemplo de configuración de este archivo podría ser:

```
## IP Estatica
auto eth0
iface eth0 inet static
address 192.168.1.1
gateway 192.168.1.1
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
dns-nameservers 192.168.1.1 8.8.8.8
# el 8.8.8.8 es un servidor de nombre gratuito de google y es
     opcional
```

*Ejemplo de configuración de interfaces obtenido de [Documentación de Ubuntu] (recomendado entrar para profundizar)*

Configuración del cliente DHCP

La parte más complicada, estaba del lado del servidor por supuesto, en donde tenemos que configurar todos los parámetros deseados para que provea de direcciones IP a nuestra red, en el caso de los equipos clientes que corran con Ubuntu, únicamente tendremos que instalar el CLIENTE DHCP y modificar el archivo de las interfaces de red (/etc/network/interfaces) para que la interfaz conectada a nuestra red, se configure de manera dinámica.

- Primero ejecutamos el comando para instalar el cliente dhcp:

```
sudo apt-get install isc-dhcp-client
```

- En Segundo término, debemos configurar la tarjeta de red para obtener una dirección dinámica:

```
nano /etc/network/interfaces
```

colocando en el archivo (en el caso de que a la red tengamos conectada la interfaz eth0):

```
auto lo eth0
iface eth0 inet dhcp
iface lo inet loopback
```

- Por ultimo, simplemente reiniciamos los servicios de red:

```
sudo /etc/init.d/networking restart
```

- Se sugiere probar la configuración seleccionada con el comando “ifconfig”

## Paquetes IP

Si hay un usuario operando un equipo A que desea enviar información a través de la red a otro usuario destinatario de un equipo B, el usuario interactúa con las aplicaciones, las que manejan protocolos de más alto nivel, la información se transmite a protocolos de más bajo nivel en ese equipo donde cada capa interviniente en el proceso

transforma o encapsula los datos de tal modo que sean inteligibles para los protocolos de esa capa, y los transmite a una capa inferior. Cuando se llega al medio físico, toda la cadena de información a enviar se transmite en forma de flujos de bits al equipo B, y son los protocolos instalados en el equipo B quienes se encargan de ir desmenuzando la información antes encapsulada.

Los datos llegan del medio físico y se transmiten de capa en capa en el orden inverso al que se transmitieron en el equipo emisor, donde cada capa extrae la información que necesita para leer los datos, los desencapsula para que los comprenda la capa superior que a su vez realizará las mismas acciones hasta llegar al nivel de aplicación, en donde la información ya habrá sido descifrada y preparada para que el usuario destinatario la comprenda.

La información que puede ser entendida por los protocolos de una capa se lee en forma de una secuencia de datos que es fragmentada para su correcta interpretación, a esa cadena de datos se le da el nombre de paquete de datos.

A nivel básico, un paquete de datos está compuesto por tres elementos:

- una **cabecera**: que contiene generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor.
- el **área de datos** (*payload*): que contiene los datos que se desean trasladar.
- la **cola** (*trailer*): que comúnmente incluye código de detección de errores.

## Campos de un paquete IP

Los paquetes son la Unidad de Datos del Protocolo (PDU) de la capa de red, generalmente, cada capa emisora de un protocolo toma la PDU de una capa superior, y lo codifica dentro del área de datos. A medida que se transmite, la capa recibe la PDU de su capa par, recupera el área de datos y la transmite a una capa superior, que procede de igual manera. Por esto, las PDU tiene encapsuladas, en su área de datos, otras PDU.

El protocolo de red IP solo tiene cabecera, ya que no realiza ninguna comprobación sobre el contenido del paquete. Sus campos se representan siempre alineados en múltiplos de 32 bits. Los campos son, por este orden:

- ***Versión**: 4 bits, se usa la versión 4 (IPv4), y ya está en funcionamiento la versión 6. Este campo permite a los routers discriminar si pueden tratar o no el paquete.*

- ***Longitud de cabecera** (IHL): 4 bits, indica el número de palabras de 32 bits que ocupa la cabecera. Esto es necesario porque la cabecera puede tener una longitud variable.*

- ***Tipo de servicio**: 6 bits (+2 bits que no se usan), en este campo se pensaba recoger la prioridad del paquete y el tipo de servicio deseado, pero los routers no hacen mucho caso de esto y en la práctica no se utiliza. Los tipos de servicios posibles son:*

  - ***D** (Delay): menor retardo, por ejemplo: para audio o vídeo.*

  - ***T** (Throughput): mayor velocidad, por ejemplo: para envío de ficheros grandes.*

- ***R*** *(Reliability): mayor fiabilidad, para evitar (en la medida de lo posible) los reenvíos.*

- ***Longitud del paquete****: 16 bits, como esto lo incluye todo, el paquete más largo que puede enviar IP es de 65535 bytes, pero la carga útil será menor, porque hay que descontar lo que ocupa la propia cabecera.*

- ***Identificación****: 16 bits, es un número de serie del paquete, si un paquete se parte en pedazos más pequeños (se fragmenta) por el camino, cada uno de los fragmentos llevará el mismo número de identificación.*

- ***Control de fragmentación****: son 16 bits que se dividen en:*

  - ***1 bit vacío****: sobraba sitio.*

  - ***1 bit DF*** *(dont't fragment): si vale 1, le advierte al router que este paquete no se corta.*

  - ***1 bit MF*** *(more fragments): indica que este es un fragmento de un paquete más grande y que, además, no es el último fragmento.*

  - ***Desplazamiento de fragmento****: es la posición en la que empieza este fragmento respecto del paquete original.*

- ***Tiempo de vida****: 8 bits, en realidad se trata del número máximo de routers (o de saltos) que el paquete puede atravesar antes de ser descartado. Como máximo 30 saltos.*

- ***Protocolo****: 8 bits, este campo codifica el protocolo de nivel de transporte al que va destinado este paquete. Está unificado para todo el mundo en Números de protocolos[1] por la Internet Assigned Numbers Authority (IANA).*

- ***Checksum de la cabecera****: 16 bits, aunque no se comprueben los datos, la integridad de la cabecera sí es importante, por eso se comprueba.*

- ***Direcciones de origen y destino****: 32 bits cada una; son las direcciones IP de las estaciones de origen y destino.*

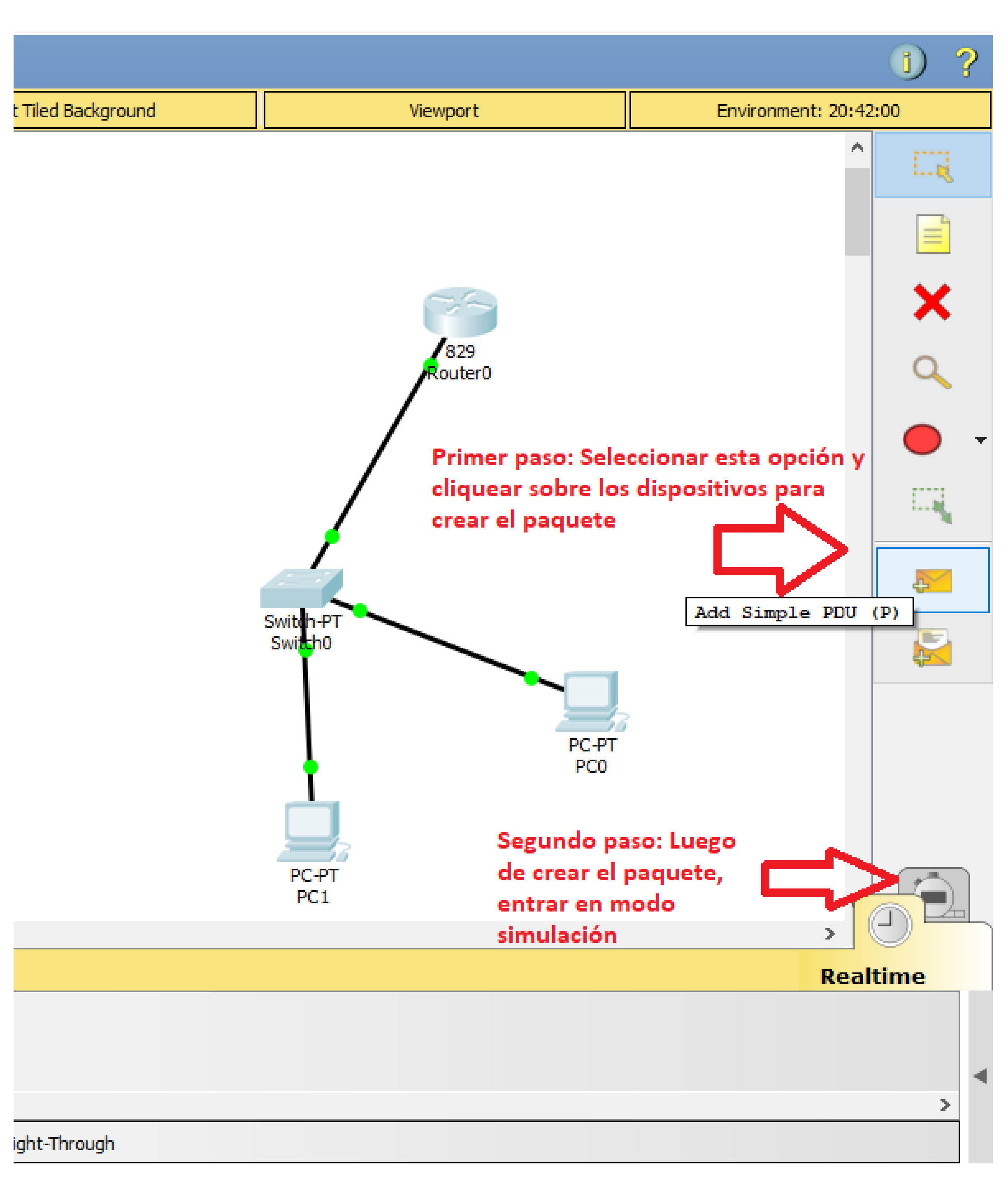
- ***Opciones****: esta parte puede estar presente o no, de estarlo su longitud máxima es de 400 bytes.*

*Información extraída de Wikipedia*

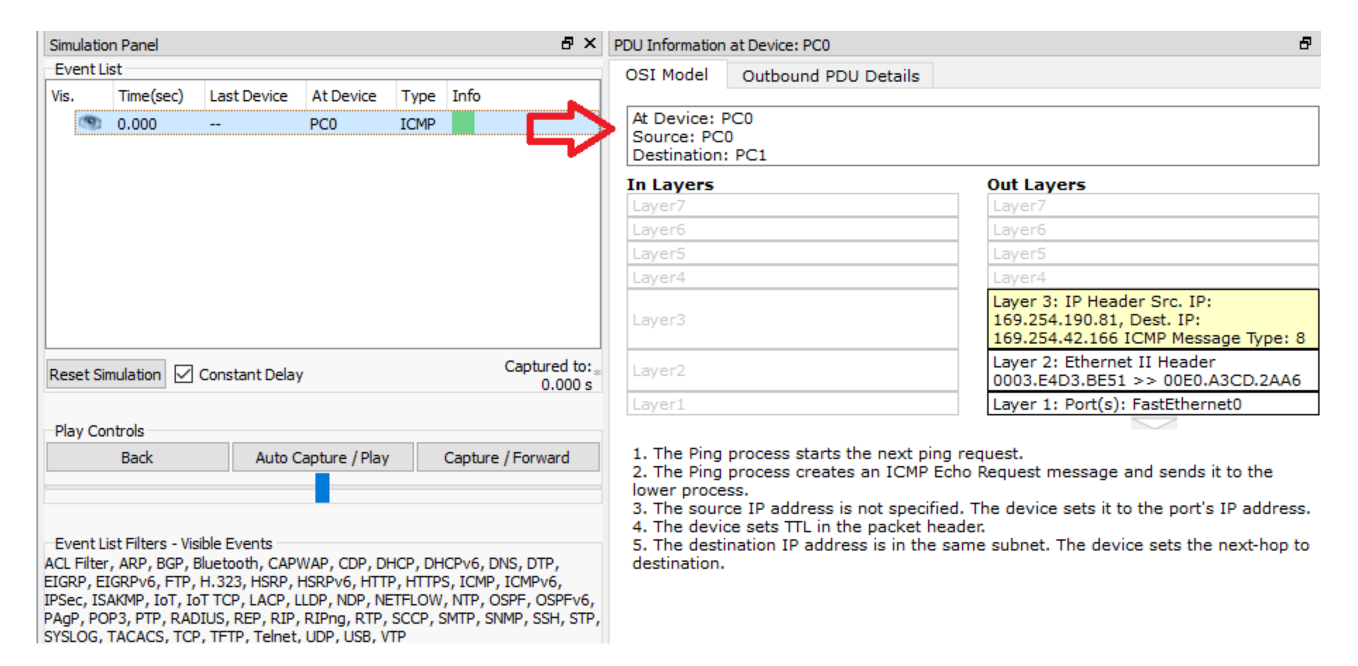
## Práctica visualizando paquetes desde el Packet Tracer

Anteriormente ya se ha trabajado con este software de simulación de redes en esta misma guía para visualizar los datos correspondientes a las tramas de datos de la capa de enlace. Sin embargo, si nos vamos un poco más en detalle, podemos visualizar la información que se guarda en los campos de los paquetes IP que se envían de un equipo a otro, realizando el mismo procedimiento anterior; consideremos para este caso, una pequeña red de dos computadoras conectadas a un conmutador, y dicho conmutador conectado a un enrutador. Hacemos clic en el ícono indicado en la imagen para crear un

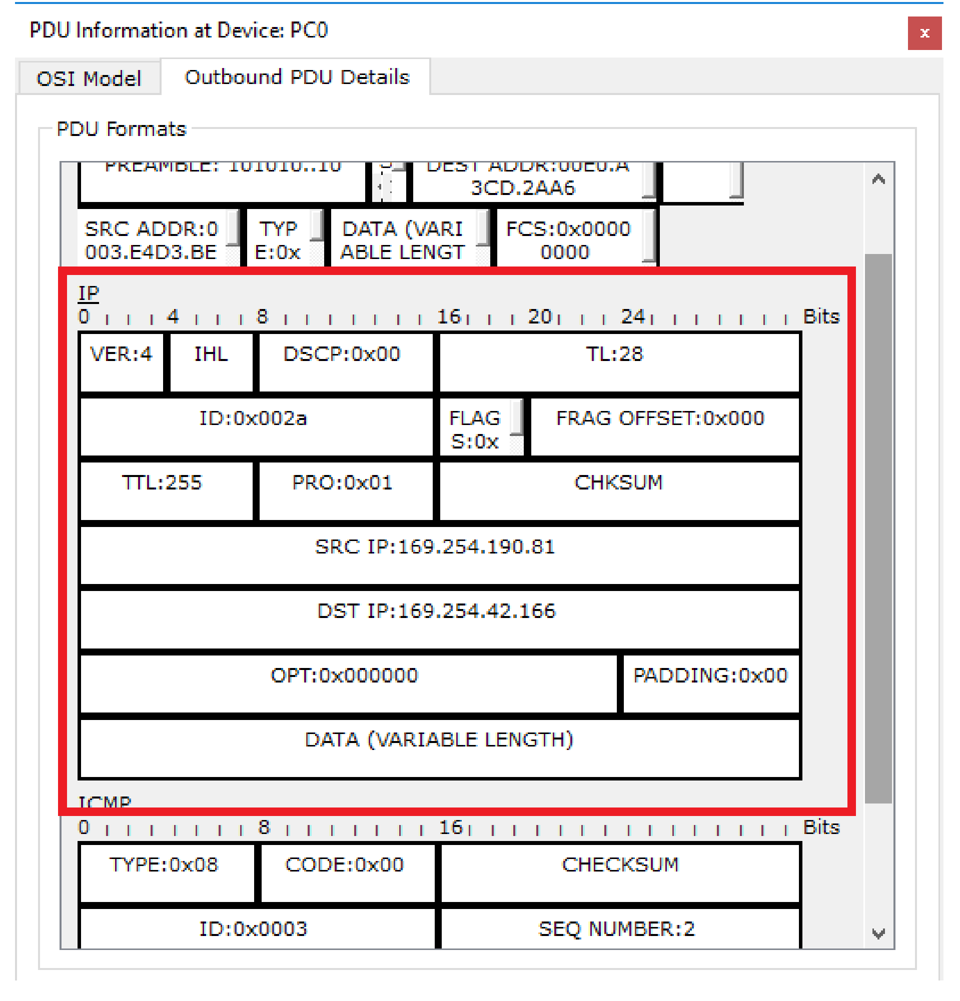
PDU simple, luego de marcada dicha opción cliquearemos sobre un equipo (origen del paquete) y luego en otro (destino del paquete):




Luego de esto, debemos entrar al modo de simulación, como se indica en la imagen más arriba, a través de dicha opción se accede al panel de simulación, desde donde podremos ver la lista de paquetes creados, en este caso práctico, uno sólo, al hacer doble clic sobre él, podremos acceder a más detalles. En la imagen siguiente podrá verse todo el panel de simulación y la pestaña emergente luego de seleccionar el paquete deseado:




Si desde la ventana emergente con la información del paquete, seleccionamos la pestaña “Outbound PDU Details”, entonces accederemos a ver cómo es el paquete de red armado por el PC0 para enviarlo al PC1:




En este momento, ya estamos en condiciones de analizar este apartado, inmediatamente vemos que el paquete en su campo de versión tiene un 4, es decir, que es un paquete de protocolo IPv4.

- La cabecera IHL nos indica que las palabras tendrán una longitud de 32 bits.
- Los campos “TL” y “TTL” reflejan el tiempo de vida, en este ejemplo el paquete tiene un “TL” de 28, es decir que para este caso el paquete podrá mantenerse pasando hasta por 28 routers intermedios entre origen y destino; también se especifica el “TTL” o tiempo de vida

máximo del paquete en la red, en este caso hasta 255 segundos (cabe destacar que Se requiere que cada dispositivo que recibe un paquete disminuya el valor de TTL en al menos 1 independientemente de si el procesamiento tomó menos de un segundo).

- El dato “FLAGS” indica el control de fragmentación del paquete, el primer bit siempre está en cero, el segundo (en este caso también está en cero) indica si puede o no fragmentarse, en este caso tiene un 0, e indica que el paquete puede ser fragmentado (un 1 indicaría que no); el tercer bit indica si hay o no más fragmentos, un 0 indicaría que el paquete es el último fragmento o que no hay más paquetes faltantes de recibir que sean otros fragmentos de la información inicialmente enviada, un 1 (como en este caso de ejemplo) indica que el paquete no es el último fragmento y que se deben esperar más.
- El campo “OFFSET” nos está indicando el desplazamiento, en este caso nos indica que la posición de este fragmento es 0 respecto al paquete original.
- El “IDENTIFICADOR” del paquete en este caso notamos que es 0x002a, es decir, todos los fragmentos que se envíen de un mismo paquete deberían llevar ese mismo identificador. Tanto el desplazamiento como el identificador, son esenciales para que el equipo destino pueda reordenar los fragmentos y armar el paquete de datos original en caso de que por problemas de red, interferencia o la causa que fuera, los fragmentos se desordenen en el camino (nótese que puede ocurrir que un primer fragmento se demore por problemas de red o llegue corrupto, se vuelva a solicitar y llegue nuevamente después que se haya enviado un segundo o tercer fragmento, entonces el equipo debe ponerlo en su lugar antes de re armar el paquete).
- El dato “PROTOCOLO” nos indica el tipo de protocolo del paquete, en este caso de ejemplo, “0x01” indica que es un paquete ICMP, si fuese por ejemplo 0x06 indicaría que es un paquete TCP, o un valor de 0x11 nos indicaría que es UDP.
- Los datos de dirección de origen y de destino son como podremos imaginar, las direcciones lógicas de los dispositivos de origen y de destino del paquete.
- El “CHECKSUM” es otro campo muy importante, y nos sirve para verificar que el paquete esté recibido en forma correcta, checksum proporciona un método para verificar que el encabezado no se haya dañado cuando se transmite de un dispositivo a otro. Para explicar su función sin entrar en los cálculos, se deriva un valor de suma de comprobación del contenido del encabezado en el origen y se vuelve a calcular en el destino; si estos valores no coinciden, el paquete será descartado. Debido a que el contenido del campo TTL cambia de un dispositivo a otro, la suma de comprobación se vuelve a calcular en cada dispositivo y se restablece en el encabezado.

## Protocolo ICMP

Su significado es “Protocolo de Mensajes de Control de Internet” y es un protocolo de soporte en el conjunto de protocolos de Internet, se lo considera un sub protocolo para transporte y detección de errores que funcionan sobre el protocolo IP. Los dispositivos de red, incluidos los enrutadores , lo usan para enviar mensajes de error e información operativa que indique, por ejemplo, que un servicio solicitado no está disponible o que no se pudo contactar con un host o enrutador. ICMP difiere de los protocolos de transporte como TCP y UDP en que normalmente no se usa para intercambiar datos entre sistemas,

ni es empleado regularmente por las aplicaciones de red del usuario final (con la excepción de las aplicaciones “ping” que ya hemos utilizado anteriormente y “traceroute”, ambas trabajan sobre el protocolo ICMP).

### *Practicando con el comando Traceroute*

Además del comando PING, otra interesante herramienta que trabaja sobre el protocolo ICMP es “traceroute” (nombre del comando en Linux) o “tracert” (nombre del comando en Windows. Este comando permite enviar un paquete con destino a una dirección IP o nombre de dominio (que se traduce a una dirección IP gracias al servicio DNS). Ingresando el comando en una terminal podremos visualizar la dirección de cada enrutador por el que pasa nuestro paquete hasta llegar a destino. Además, nos muestra el tiempo de demora en milisegundos que le lleva llegar a cada enrutador.

Algunos routers pueden estar configurados para no mostrar su información abiertamente, manteniendo oculta su dirección e imposibilitando al usuario conocer con exactitud el camino que recorre el paquete hasta llegar a destino. A continuación se muestra una imagen intentando enviar un paquete desde el equipo donde se escribe a un servidor de Google, para ello, se podría utilizar la IP pública del servidor, pero como nos es desconocida, simplemente se ingresa *“`tracert www.google.com`”* y el sistema muestra en pantalla su dirección IP, y los saltos que efectúa el paquete hasta llegar a destino:

```
Símbolo del sistema

Traza a la dirección www.google.com [64.233.190.104]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  192.168.2.1
  2     4 ms     4 ms     4 ms  10.14.2.1
  3     4 ms     4 ms     4 ms  10.10.33.1
  4    25 ms    28 ms    26 ms  10.10.33.2
  5     5 ms     5 ms     5 ms  190.0.150.1
  6     *        *        *     Tiempo de espera agotado para esta solicitud.
  7     5 ms     5 ms     5 ms  asr3cor6-bexxx-1603.antel.net.uy [200.40.177.187]
  8     6 ms     7 ms     6 ms  ibb2cor3-be200-1603.antel.net.uy [200.40.177.186]
  9    34 ms    32 ms    32 ms  192.168.2.217
 10    23 ms    25 ms    22 ms  192.168.1.90
 11    38 ms    36 ms    29 ms  192.168.2.166
 12    37 ms    36 ms    36 ms  216.239.50.31
 13    42 ms    42 ms    42 ms  108.170.238.209
 14     *        *        *     Tiempo de espera agotado para esta solicitud.
 15     *        *        *     Tiempo de espera agotado para esta solicitud.
 16     *        *        *     Tiempo de espera agotado para esta solicitud.
 17     *        *        *     Tiempo de espera agotado para esta solicitud.
 18     *        *        *     Tiempo de espera agotado para esta solicitud.
 19     *        *        *     Tiempo de espera agotado para esta solicitud.
 20     *        *        *     Tiempo de espera agotado para esta solicitud.
 21     *        *        *     Tiempo de espera agotado para esta solicitud.
 22     *        *        *     Tiempo de espera agotado para esta solicitud.
 23     *        *        *     Tiempo de espera agotado para esta solicitud.
 24    42 ms    42 ms    42 ms  gsademo23.google.com [64.233.190.104]

Traza completa.
```

Observamos que, el paquete en primer lugar pasa por un router, que lo identifica a nivel local con la dirección privada 192.168.2.1, luego encontramos que pasa por routers con direcciones de clase A con un muy bajo nivel de demora (4ms y 26 ms) y luego ya pasa por un router con una dirección de clase B con una demora de 5ms (debido a las clases de las direcciones, asumimos que estos pasos son por enrutadores de una red grande de la institución a través de la cual está conectado el equipo), luego pasa por servidores de ANTEL (nuestra ISP) y después de ello hay varios saltos por routers o

direcciones públicas de clase C. Posteriormente hay varios saltos por routers cuya información se nos oculta y el tiempo de espera aparentemente se ha agotado, con el tiempo de espera por defecto en traceroute, que son 5 segundos.

El tiempo de espera puede cambiarse con el modificador "-w [TIEMPO]" de el comando (se sugiere observar los modificadores ingresando "`tracert /?`" (Windows).

## Enrutamiento

El enrutamiento o encaminamiento de la información es otra de las funcionalidades que brinda la capa 3 o capa de red, a la comunicación en redes de computadoras. Existen dispositivos que se encargan de esto y son los enrutadores o routers. Cuando trabajamos con redes de área local o subredes, no necesitamos de dispositivos para trazar caminos entre las terminales conectadas dentro del ámbito local, sin embargo, cuando tenemos subredes diferentes, sucede que los equipos pertenecientes a una subred no pueden acceder de manera directa a otros dispositivos si no cuentan con un dispositivo intermedio que encamine dicho paquete. De dicho encaminamiento se encarga un router, por lo cual este tipo de dispositivos es esencial en redes de área extendida y en casi cualquier red de una dimensión considerable. Podríamos decir que todas las redes MAN, WAN y por supuesto, en Internet necesitamos inevitablemente de enrutadores que se encarguen de interconectar las redes.

El encaminamiento no sólo consiste en encontrar una ruta para el viaje de los datos, sino la mejor ruta o la más eficiente; el criterio para encontrar dicha ruta varía, y va a depender de los protocolos a utilizar. Puede considerarse como mejor ruta a la más cercana, a la que tiene menos saltos (menos routers intermedios entre el dispositivo de origen y el de destino) o el más rápido en términos de demora de dichos routers.

En pocas palabras, podríamos definir al encaminamiento como la **búsqueda de un camino para los paquetes, entre todos los posibles en una red cuyas topologías poseen una gran conectividad. Así, encaminar un paquete es la fase de enviar dicho paquete basándose en una IP de destino.**

### Funcionamiento de un Router

Si entendemos por subred a un conjunto de terminales conectados y configurados de tal modo que, pueden establecer comunicación sin necesidad de un enrutador, es decir, simplemente utilizando dispositivos para establecer la conexión física, como puentes o switches, sale en evidencia que la utilidad de los routers es permitir la conexión entre equipos de diferentes subredes. Los enrutadores son los dispositivos encargados de esta trarea, para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen.

Con arreglo a esta información reenvía los paquetes a otro enrutador o bien al equipo de destino. Cada enrutador se encarga de decidir el siguiente salto en función de su tabla de reenvío o tabla de encaminamiento, la cual se genera mediante protocolos que deciden cuál es el camino más adecuado o corto.

Los enrutadores, utilizan tablas de enrutamiento para almacenar las rutas a los diferentes destinos. Dichas tablas, son documentos electrónicos, y son imprescindibles

para que el dispositivo conozca los caminos hacia los nodos que tiene accesibles, entendiéndose por nodos, a otros enrutadores o bien a equipos finales.

En las imágenes presentadas a continuación, podremos ver una tabla de enrutamiento mostrada desde la línea de comandos de Windows, ingresando el comando `route print`:

```
Símbolo del sistema

C:\Users\vicmn>route print
===========================================================================
ILista de interfaces
 20...d0 bf 9c 95 d6 8b ......Realtek PCIe FE Family Controller
 10...c6 8e 8f 59 f0 4f ......Microsoft Wi-Fi Direct Virtual Adapter #2
 11...c4 8e 8f 59 f0 4f ......Microsoft Wi-Fi Direct Virtual Adapter #3
 17...c4 8e 8f 59 f0 4f ......Realtek RTL8723BE 802.11 b/g/n Wi-Fi Adapter
  7...c4 8e 8f 59 f0 50 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      10.27.156.1     10.27.156.53     55
      10.27.156.0    255.255.252.0      En vínculo      10.27.156.53    311
     10.27.156.53  255.255.255.255      En vínculo      10.27.156.53    311
    10.27.159.255  255.255.255.255      En vínculo      10.27.156.53    311
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    331
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    331
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1    331
        224.0.0.0        240.0.0.0      En vínculo      10.27.156.53    311
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
  255.255.255.255  255.255.255.255      En vínculo      10.27.156.53    311
===========================================================================
Rutas persistentes:
  Ninguno
```

*Por ser los elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:*

- *Reenvío de paquetes: cuando un paquete llega al enlace de entrada de un router, éste tiene que pasar el paquete al enlace de salida apropiado. Una característica importante de los encaminadores es que no difunden tráfico difusivo (es decir, no proporcionan broadcasting, no permiten que un equipo envíe a muchos otros de manera simultánea).*

- *Encaminamiento de paquetes : mediante el uso de algoritmos de encaminamiento tiene que ser capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.*

*Por tanto, debemos distinguir entre reenvío y encaminamiento. Reenvío consiste en tomar un paquete en la entrada y enviarlo por la salida que indica la tabla, mientras que por encaminamiento se entiende el proceso de hacer esa tabla.*

*Información extraída de Wikipedia*

Existe el encaminamiento de tipo dinámico y estático. Las clases de enrutamiento pueden ser por vector distancia o por estado de enlace. Dentro de las comunicaciones y redes también existen protocolos de enrutamiento, que no deben confundirse con protocolos enrutados.

## Rutas estáticas y dinámicas

*Las rutas estáticas son gestionadas manualmente por el administrador de red, siempre que un cambio se presente en la topología de internetwork.*

*Tienen las siguientes características:*

- *Permiten la configuración manual de las tablas de enrutamiento.*
- *Las tablas no podrán ser modificadas en forma dinámica*
- *Falta de flexibilidad frente a fallas de los enlaces*
- *No son necesarios las cargas y procesos asociados a un protocolo de descubrimiento de rutas.*
- *Es fácil establecer barreras de seguridad bajo este modelo.*

*Las rutas dinámicas se actualizan automáticamente a través de un proceso de enrutamiento cuando se recibe información de la red, estos cambios son informados a los demás Routers como parte del proceso de actualización.*

*El éxito del enrutamiento dinámico depende de dos funciones básicas del Router:*

- *El mantenimiento de una tabla de enrutamiento.*
- *La distribución oportuna del conocimiento, bajo la forma de actualizaciones de enrutamiento, hacia otros Routers.*

(D.Payares y M.Fandiño, 2004)

## Enrutamiento Estático y Dinámico

**El enrutamiento dinámico** se basa en un protocolo para poder compartir el conocimiento sobre las rutas cercanas entre diferentes routers, dicho protocolo se conoce generalmente como protocolo de enrutamiento, y es el encargado de definir el conjunto de reglas a utilizar para comunicarse con enrutadores vecinos. En dicho protocolo se describe:

- Cómo se envían las actualizaciones entre routers
- Cuándo enviar las actualizaciones
- Cómo ubicar a los enrutadores destinatarios de dichas actualizaciones.

El encaminamiento dinámico revela toda la información acerca de su red con otros routers.

**El enrutamiento estático** es otro método de enrutamiento utilizado para interredes, a diferencia del método anterior, donde las tablas de ruteo son administradas y actualizadas de forma automática por un protocolo de enrutamiento, en el enrutamiento estático debe haber un administrador de redes, generalmente un ingeniero u otro operador con conocimientos avanzados que se encargue de actualizarla manualmente.

No se debe pensar por esto que, el enrutamiento estático es menos avanzado o más antiguo que el método dinámico, ambos métodos son las únicas vías existentes y utilizadas para la conexión de diferentes subredes, y presentan ventajas o desventajas dependiendo del caso. Para interredes de menor tamaño, el enrutamiento estático es más viable porque proporciona mayor seguridad a la red en cuestión, el administrador de la red puede elegir no revelar parte de la información de la red. Por otra parte, una ruta estática puede ser suficiente cuando se desea acceder a una red a través de un solo camino, evitando el gasto que conlleva el enrutamiento dinámico.

Para ser más claros, se debe tener presente la siguiente tabla comparativa:

| | Enrutamiento dinámico | Enrutamiento estático |
|---|---|---|
| Complejidad de la configuración | Por lo general es independiente del tamaño de la red | Se incrementa con el tamaño de la red |
| Conocimientos requeridos del administrador | Se requiere de un conocimiento avanzado | No se requieren conocimientos adicionales |
| Cambios de topología | Se adapta automáticamente a los cambios de topología | Se requiere la intervención del administrador |
| Escalamiento | Adecuado para las topologías simples y complejas | Adecuada para topologías simples |
| Seguridad | Es menos seguro | Más segura |
| Uso de recursos | Utiliza CPU, memoria y ancho de banda de enlace | No se requieren recursos adicionales |
| Capacidad de predicción | La ruta depende de la topología actual | La ruta hacia el destino es siempre la misma |

Imagen obtenida del siguiente Artículo de la Universidad de Venezuela.

### *Algoritmos de Enrutamiento*

Cuando tenemos enrutamiento dinámico (que también se conoce como encaminamiento adaptativo) se debe emplear un algoritmo para calcular cuál es la mejor ruta para encaminar un paquete. Los criterios para considerar una ruta como “mejor” son relativos, no obstante todo algoritmo de encaminamiento debe garantizar correctitud, robustez (debe ser tolerante a fallos para redes que perduren por años) y estabilidad.

Algoritmos por Vector de Distancias

En esta clase de enrutamiento, cada Router mantiene una tabla o vector que almacena las mejores distancias y rutas conocidas a cada destino, actualizándose con el intercambio de información con los Routers vecinos. Algunos protocolos que utilizan este algoritmo son RIP (en sus versiones 1 y 2) e IGRP.

Todo Router almacena en su tabla una entrada para cada uno de los Routers en la subred. Las entradas van almacenando la línea preferida, de acuerdo a la métrica que se esté utilizando, que puede ser teniendo en cuenta distancia física, el número de saltos, el retraso de la transmisión, el costo de la comunicación etc.

Cada router debe medir la distancia con sus vecinos, intercambiando sus tablas, las tablas vecinas son utilizas para que el enrutador pueda recalcular distancias y actualizar sus propias tablas basado en las vecinas.

Algoritmos de Estado del Enlace

Estos métodos implican que cada enrutador conozca la topología de red y los costos o retardos asociados a cada enlace, para que a partir de estos datos, pueda obtener el árbol y la tabla de enrutamiento aplicando un algoritmo que calcule el costo mínimo (Algoritmo de Dijkstra) a todo el grafo de la red.

Nota: En caso de que el lector no comprenda de lo que se trata un grafo, se recomienda leer los siguientes artículos para tener una noción de ello:

- Teoría de Grafos
- Algoritmo de Dijkstra

Un ejemplo de protocolos que utilizan estado de enlace es protocolo OSPF, del cual ya se habló previamente en el apartado de Conmutación, numeración y ruteo en redes telefónicas.

## Protocolos Enrutados y de Enrutamiento

*Existe una marcada diferencia entre protocolo enrutado y protocolo de enrutamiento. Los protocolos enrutados son los que se desplazan a través de una red. Tales como el Protocolo de control de transmisión/Protocolo Internet (TCP/IP) y el Intercambio de paquetes de internetworking (IPX). Los protocolos de enrutamiento enrutan los protocolos enrutados a través de una red, tales como:*

- *IGRP.*
- *Primero la ruta libre más corta (OSPF).*
- *Protocolo de gateway exterior (EGP).*
- *Protocolo de gateway fronterizo (BGP).*
- *Enrutamiento OSI.*
- *Red avanzada de par a par (APPN).*
- *Sistema intermedio-Sistema intermedio (IS-IS).*
- *RIP*

(D.Payares y M.Fandiño, 2004)

Dada la explicación anterior, cabe señalar que **todos los protocolos que se han mencionado anteriormente cuando se habló de enrutamiento dinámico, son protocolos de enrutamiento**, es decir, protocolos que indican al router el mecanismo a seguir para encontrar la mejor ruta a la hora de encaminar un paquete. El protocolo configurado en el router para "decirle como aprender" a cerca de otros routers es siempre un protocolo de enrutamiento. **Los protocolos enrutados por su parte son los que establecen direcciones para identificar los equipos y a las redes individuales dentro de cada red**. El protocolo IP en cualquiera de sus versiones, ya trabajado anteriormente, es un protocolo enrutado.

De esto se deduce lo que anteriormente se detallaba, que el protocolo de enrutamiento, cualquiera que sea, también utiliza protocolos enrutados para poder identificar los dispositivos y almacenar sus direcciones dentro de las tablas, o en otro

caso, ¿Cómo podrían identificarse las computadoras o routers cercanos?. Las direcciones lógicas, son direcciones de protocolos enrutados.

### *Sistemas Autónomos*

Se le llama sistema autónomo a un sistema que incluye a todos los equipos y a las redes que quedan contenidas dentro del dominio administrativo de una red de área amplia. Supongamos que una empresa tiene varios edificios o sucursales, en donde cada una de ellas se utiliza redes de área local para conectar los dispositivos. Además, la empresa tiene conectadas las diferentes redes de cada edificio utilizando enrutadores, formando así una red de área amplia. La red que abarca a todas las sucursales sería considerada un sistema autónomo.

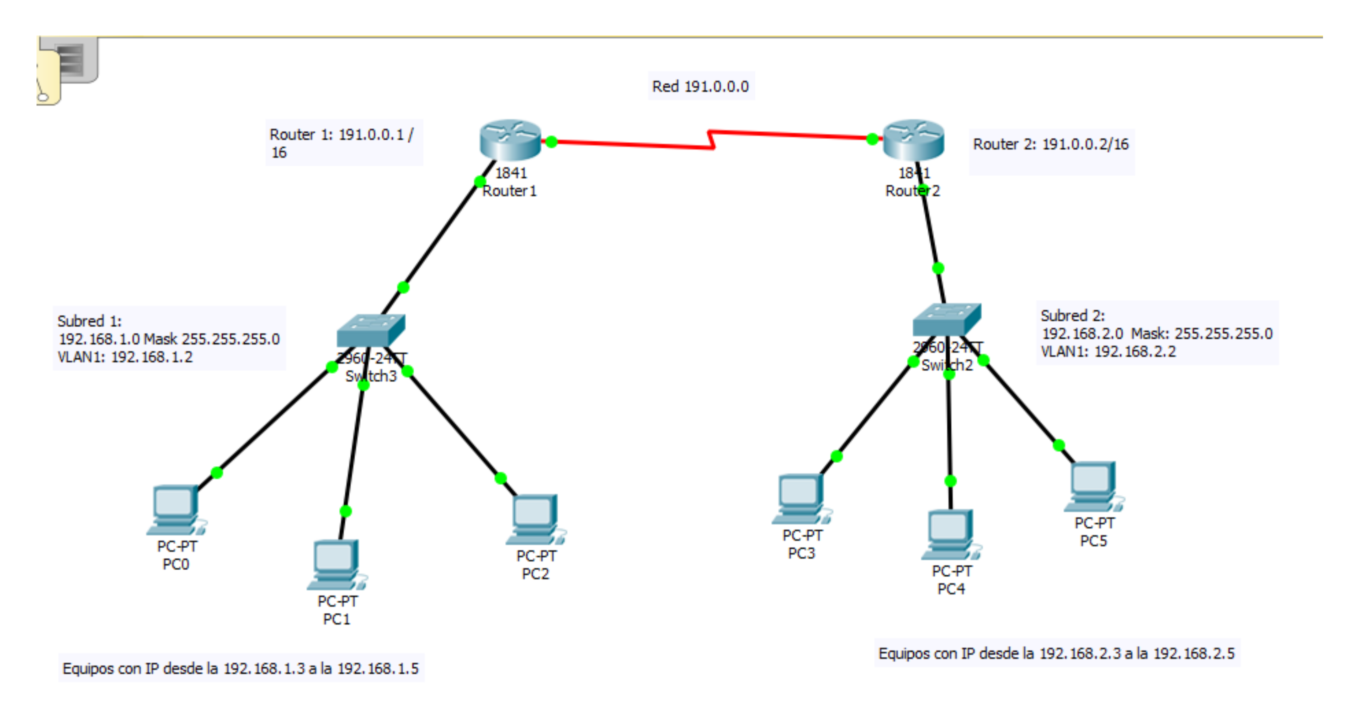
## Practicando contenidos sobre encaminamiento

### *Creación de dos redes LAN independientes con conmutadores CISCO en Packet Tracer*

Ahora que ya hemos trabajado sobre enrutamiento desde lo teórico, ha llegado el momento de ponerlo en práctica. Como el hardware de red es costoso, sobre todo si empleáramos conmutadores y enrutadores de alta calidad (como anteriormente se ha mencionado, usando dispositivos Cisco) se trabajará emulando dichos dispositivos con el software Packet Tracer. No se mostrará cómo acceder al entorno del programa y crear dispositivos porque esas actividades ya se han desarrollado en Uso del software CISCO Packet Tracer.

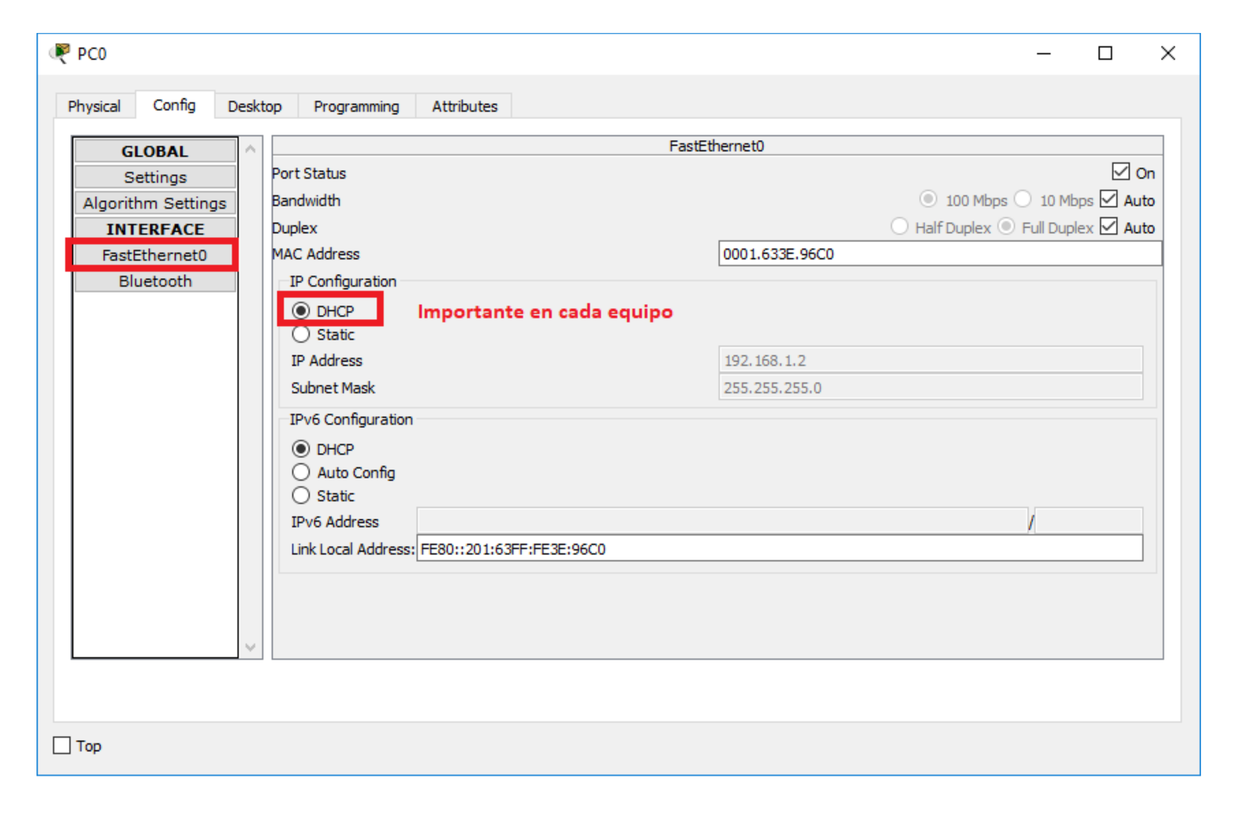
Sin embargo, vamos a abordar desde la práctica la temática antes mencionada sobre la creación de un servidor DHCP desde un switch que brinde esta funcionalidad (un switch de capa 3 como ser el Cisco 2960). Se crearán dos subredes con un switch de este tipo en cada una, y por último se trabajará con enrutamiento estático y dinámico.

El objetivo, es tener dos redes conectadas a través de dos enrutadores Cisco 1841 (se puede optar por otros modelos) conectados entre sí a través de un puerto serial, en un esquema como el que se puede ver en la imagen debajo:




## Creando redes LAN con switches CISCO usando DHCP

Como estamos trabajando en este ejemplo con Switches modelo 2960, podemos configurar cada switch para que ofrezca servicio DHCP a los equipos conectados. Éstos a su vez, deben estar configurados para que sus interfaces de red tomen direcciones obtenidas por DHCP, para ello, debemos configurar cada equipo como se ve en la siguiente imagen:




Por otro lado, cabe destacar que la primer subred será de la forma 192.168.1.0 mientras que la segunda será 192.168.2.0, ambas con máscara 255.255.255.0, por lo que

los equipos conectados deberán tomar direcciones de IP en el rango que configuremos cada switch correspondiente a su subred. En primer lugar, debemos entonces configurar cada Switch, en cada caso conectaremos cada PC a su switch correspondiente utilizando cable par trenzado convencional a puertos de red del switch desde el segundo en adelante (este orden no es obligatorio, pero para ser prolijos seguimos esa regla) y dejamos el primer puerto para conectar por cable par trenzado cada switch a su respectivo router. Después configuraremos los conmutadores (switches), los pasos a seguir no son complicados, pero debemos prestar atención en lo que hacemos ya que trabajaremos por línea de comandos. Debemos ir a la configuración de cada switch en la pestaña “CLI”, y realizar las siguientes actividades (en cada uno de los switches):

- Configuración de IP para la VLAN (en este caso usaremos sólo una red virtual en cada switch)
- Configuración del Pool de direcciones DHCP, brindando configuración de IP y máscara para la red y configurando la IP del router por defecto (default router).
- Configurar la puerta de enlace predeterminada
- Guardar la configuración y salir del menú de configuración.

Entrando al menú de configuración por línea de comandos en cada switch, simplemente debemos ingresar los comandos para entrar a configurar en modo privilegiado, ellos son:

```
enable
```

Y luego

```
configure terminal
```

Luego pasamos a configurar la VLAN (por defecto se suele llamar Vlan 1, y todas las salidas de red en Packet Tracer pertenecen a dicha Vlan, aunque esto sabemos que podemos cambiarlo), le asignamos la IP con la máscara correspondiente, en la imagen debajo estamos posicionados sobre el conmutador de la **segunda subred**, por lo que trabajaremos con la dirección 192.168.2.2 (Tomamos la segunda dirección de la red para dejar libre la primera para a futuro conectar el router) y máscara 255.255.255.0 para referirnos a la interfaz de esa red virtual, los comandos son :

```
interface Vlan 1

ip address 192.168.2.2 255.255.255.0

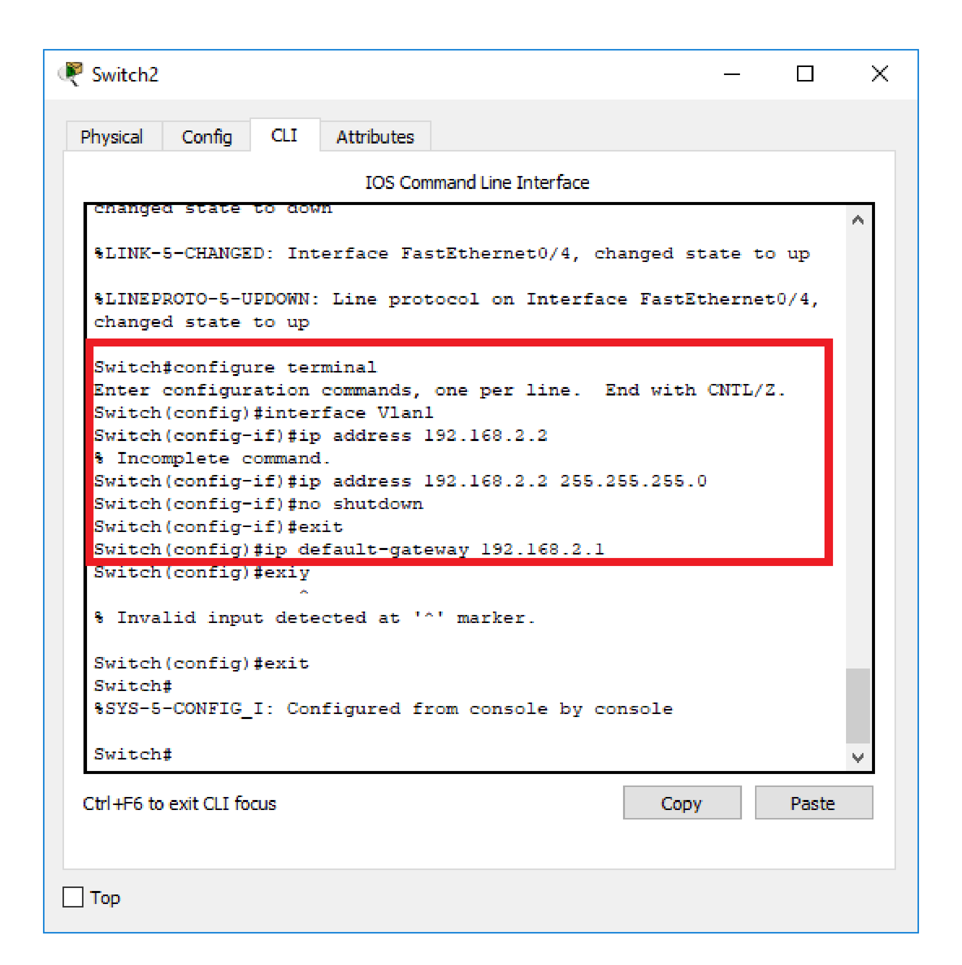
no shutdown

exit
```

Luego de configurar los parámetros de la VLAN (en el caso del ejemplo, la segunda) configuramos la puerta de enlace predeterminada, que **para esta segunda red, será el segundo router**, es decir, la 192.168.2.1, el comando es:

```
ip default-gateway 192.168.2.1
```

Debajo puede observarse una imagen con los comandos señalados para realizar estas configuraciones.




Ahora resta configurar el servidor DHCP para cada switch, entonces, para cada caso, debemos crear un pool DHCP y asignar IP de la red y la IP para el switch, además de la configuración DNS (opcional), a modo de ejemplo, en el switch correspondiente a la **segunda subred**, se deben ingresar los siguientes comandos (detallados en la captura de pantalla que aparece debajo):

```
ip dhcp pool VLAN1

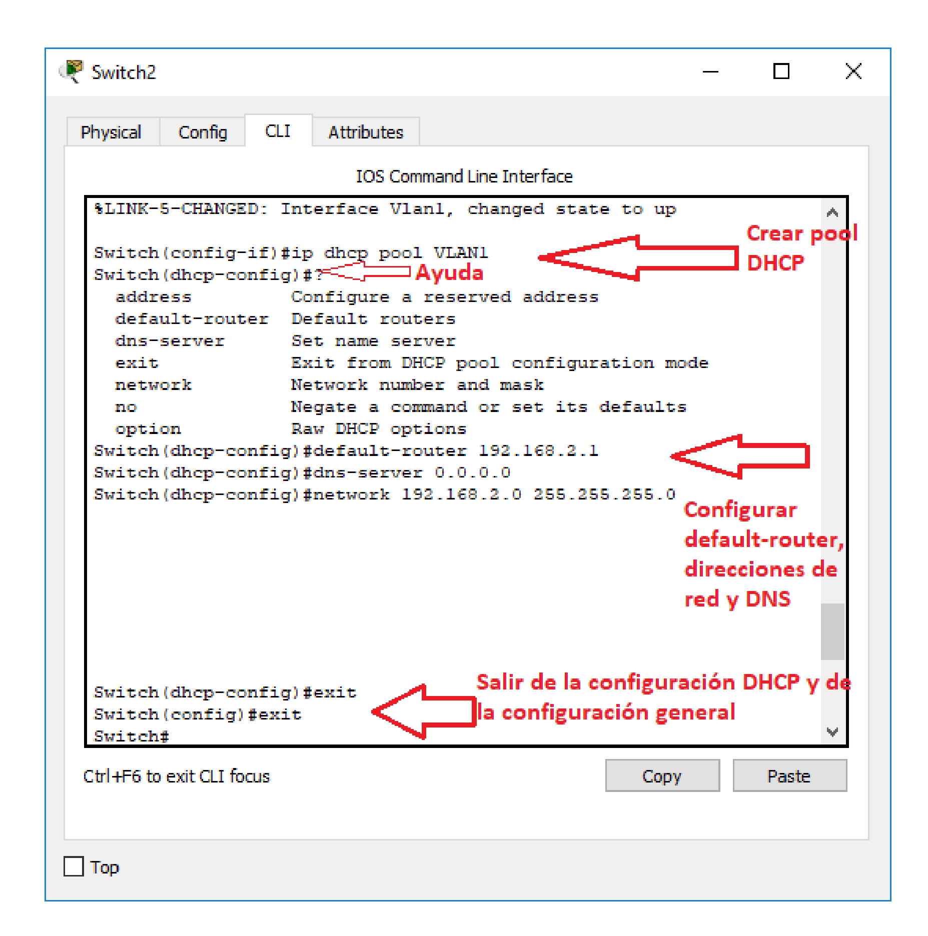
default-router 192.168.2.1

dns-server 0.0.0.0

network 192.168.2.0 255.255.255.0

exit

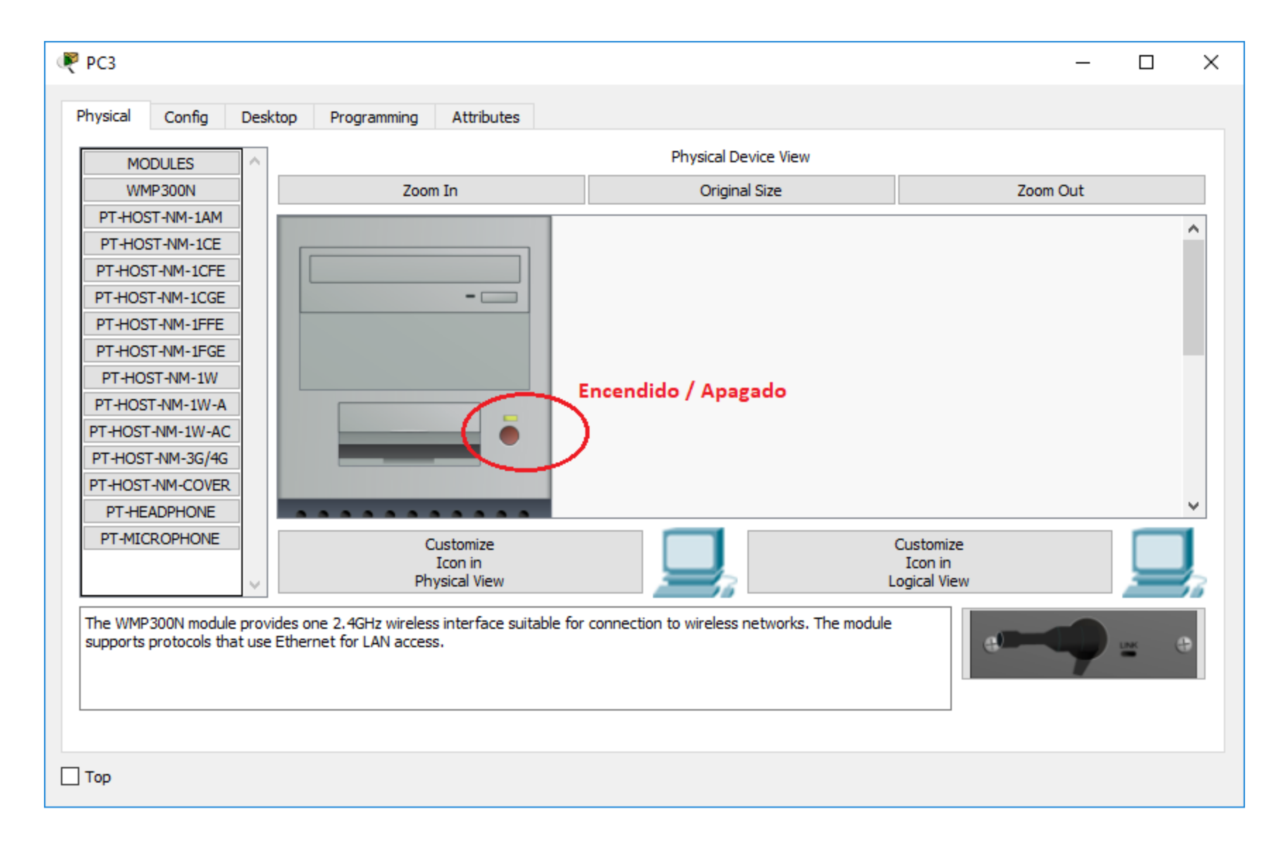
exit
```



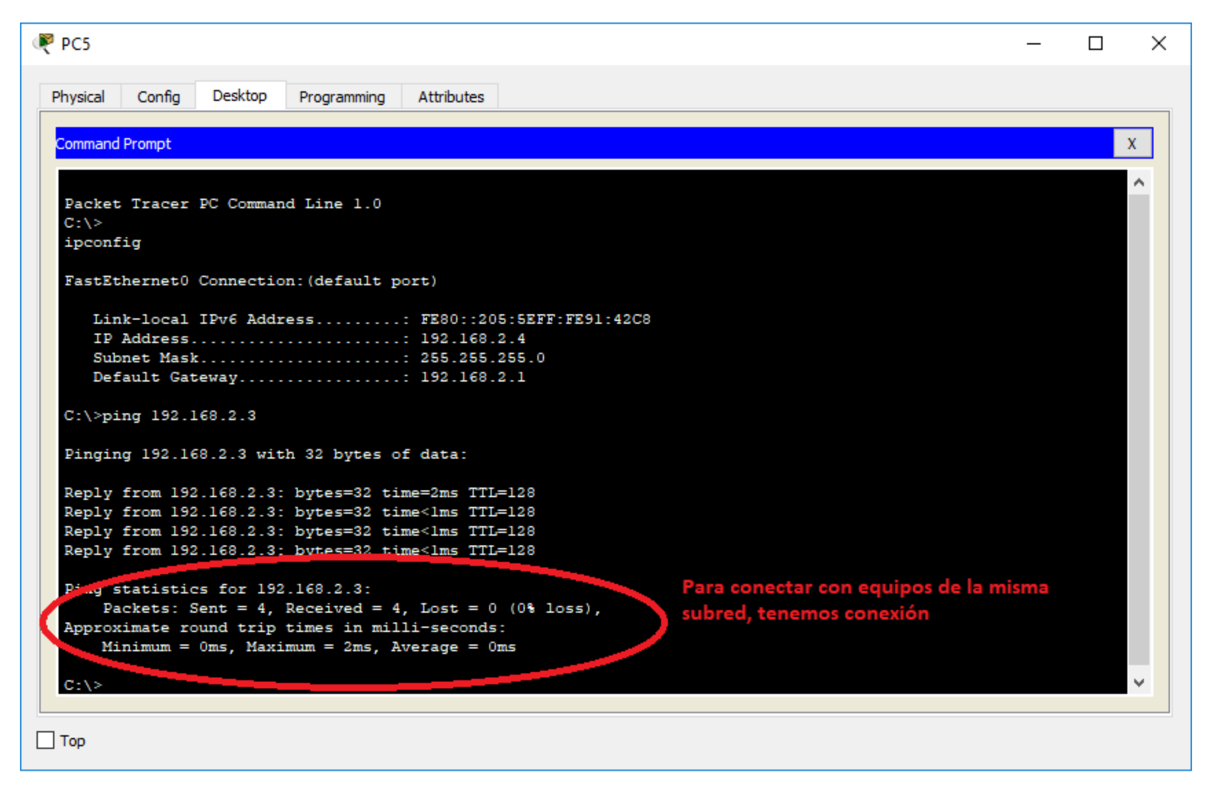

La razón por la que ingresamos “exit” dos veces es porque en principio debemos salir de la configuración DHCP, y luego de la configuración global.

Una vez ingresamos los comandos debemos dar ENTER para que el switch guarde la configuración, debemos visualizar esto en pantalla, y el sistema nos debería indicar que se ha creado el servidor con la IP correspondiente. **Todo el procedimiento debería repetirse para la otra subred, la cual tendrá la dirección 192.168.1.0 en lugar de la ya seleccionada 192.168.2.0, los ajustes correspondientes en el respectivo switch, se deberán realizar teniendo en cuenta este cambio.**

Por último, cabe señalar que si a los equipos que tenemos conectados en cada conmutador no los hemos configurado aún para que sus interfaces soliciten direcciones DHCP, debemos hacerlo y por último reiniciar cada equipo, es decir, apagarlo y volverlo a encender, para que el switch correspondiente lo pueda configurar de acuerdo a su servidor DHCP, que lo hemos ajustado por consola, para apagar un equipo simplemente debemos ir a la pestaña de su estructura física, y presionar sobre el botón de apagado:




Para comprobar que exista conexión, simplemente utilizaremos el comando PING e intentarnos conectar hacia otro equipo, en este caso en la imagen inferior, veremos que sobre el PC5, conectado en la segunda subred, tenemos una IP asignada por el servidor DHCP configurado en el switch, y satisfactoriamente podemos conectarnos al PC4, que es el que posee la dirección 192.168.2.4:



Como no hemos configurado los routers para que exista encaminamiento entre las diferentes subredes, intentaremos enviar un paquete hacia un equipo de la primera subred, y podremos observar que el mismo nunca llega, y que el comando PING nos indica que el destino es inaccesible:

PC5

Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=2ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

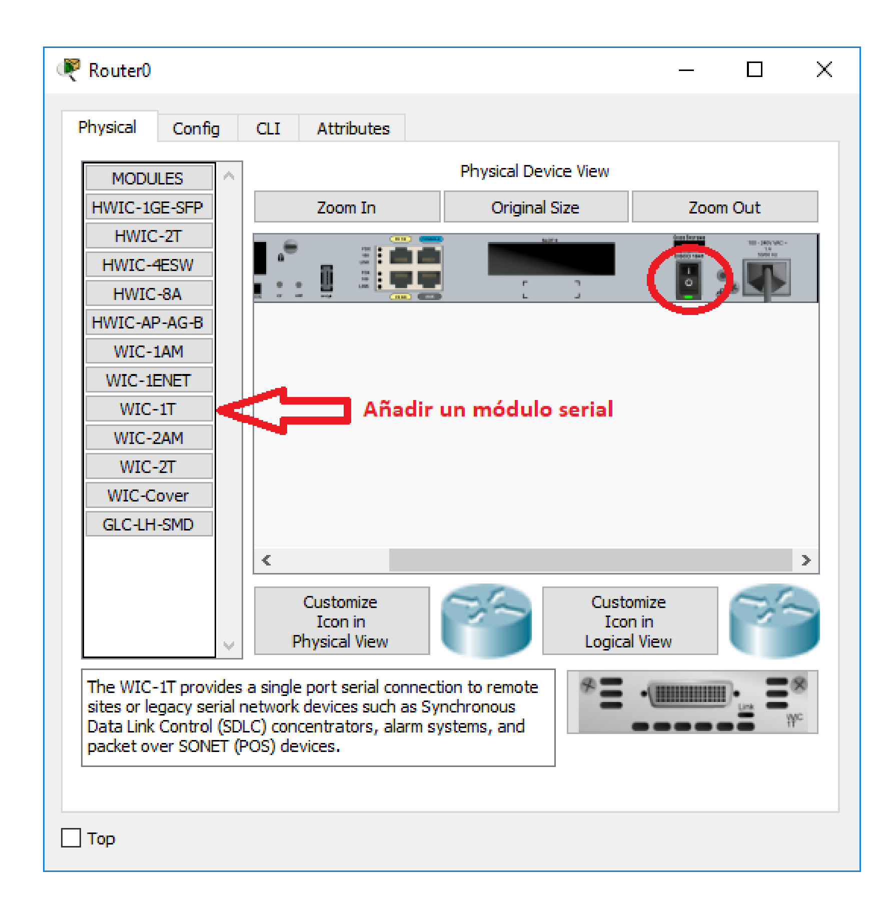
Para acceder a los equipos de otra subred, sin tener ruteo, NO TENEMOS CONEXIÓN

Top

### *Encaminamiento estático con routers CISCO en Packet Tracer*

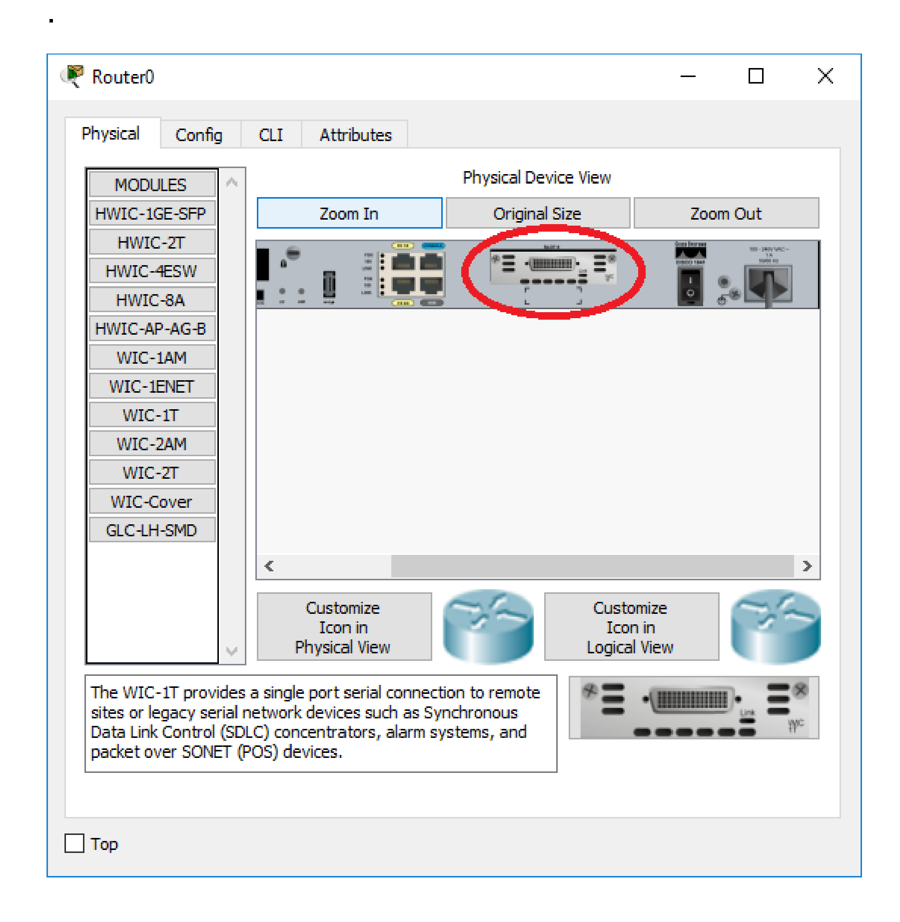
En las dos redes creadas anteriormente, vamos a necesitar un router conectado a cada switch, para que mediante una conexión entre amos routers se puedan conectar ambas subredes y así, poder tener conexión entre los equipos de las diferentes subredes. Para ello, debemos crear ambos routers y en cada caso la primera interfaz de red (FastEthernet) a la primera de su respectivo switch. A nivel físico, ambos routers deberán conectarse a través de cable serial DTE, pero sucede que, para que esto sea posible, deberemos añadir en cada router el módulo del puerto serial correspondiente. En las siguientes imágenes vemos el procedimiento:

Primero, debemos dar doble clic al router en cuestión, e ir a la pestaña de la configuración "Física", y en la lista de módulos elegimos "WIC-1T", debemos cliquear en la imagen correspondiente al router emulado el botón de apagado, ya que el módulo de hardware debe agregarse obviamente, con el router apagado:



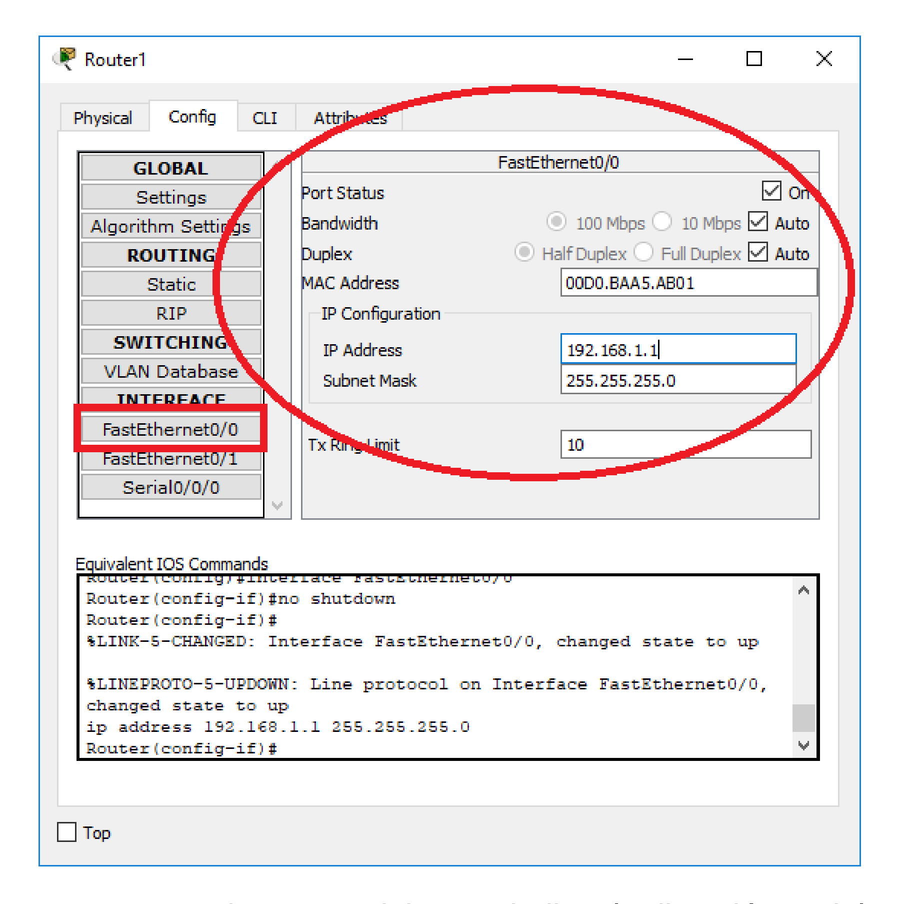

En segundo lugar, simplemente arrastramos el módulo del puerto serial hacia un puerto libre que tenga el router (se representan con rectángulos negros):

.

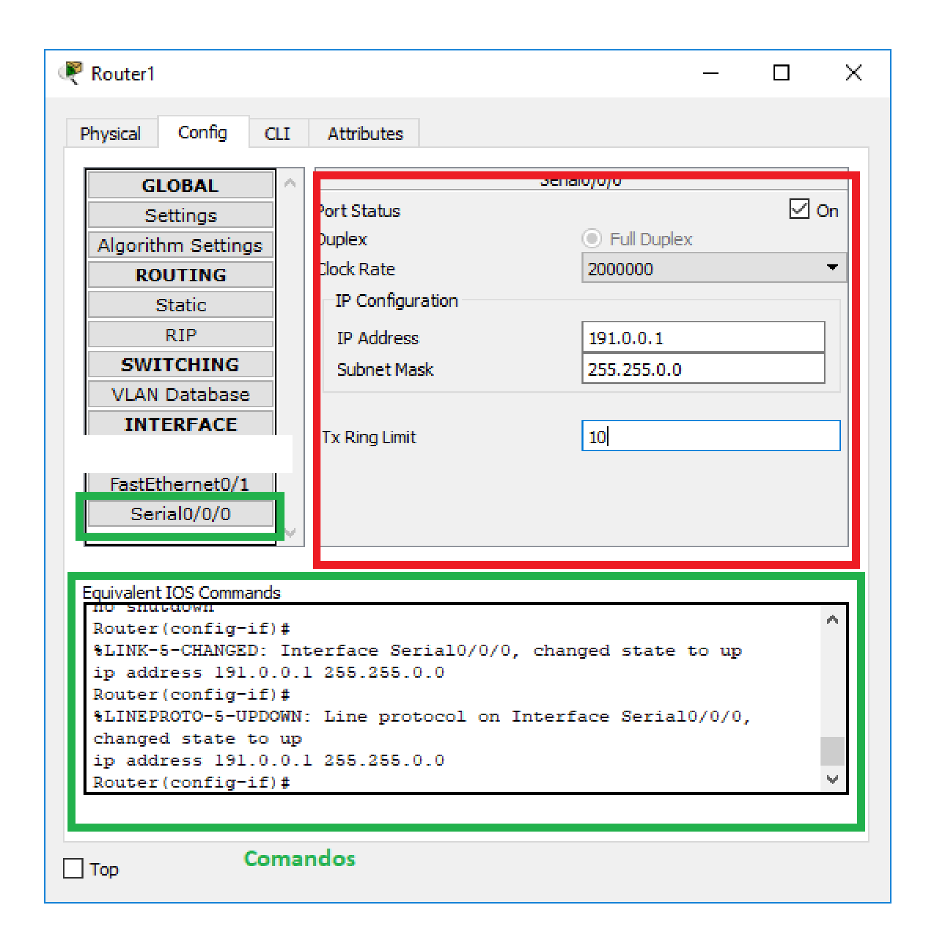


Finalizado este proceso, ya podemos conectar ambos routers a través del cable serial y empezar a configurar las tablas de ruteo. En primer lugar, vamos a activar la interfaz de red conectada al switch (la primera interfaz), e indicarle su dirección IP y máscara, en este caso será 192.168.1.1 y máscara 255.255.255.0. Tener en cuenta que, esto se va a realizar **desde el primer router, es decir, el que está conectado a la red con dirección 192.168.1.0**, los comandos correspondientes a esta configuración serían:

```
enable
configure terminal
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
```




Posteriormente, debemos indicar la dirección IP del puerto serial de este **primer router**, esto definirá la red de ambos routers, que puede diferir completamente de las direcciones elegidas para las subredes que conectan cada uno. Para este caso, hemos elegido por ejemplo la dirección 191.0.0.0 para esta red, es decir, optamos por crear una red de clase B, donde el primer router tomará en su puerto serial la dirección IP 191.0.0.1 y la máscara será 255.255.0.0, activamos su puerto serial y repetimos el proceso, como se ve en la imagen:



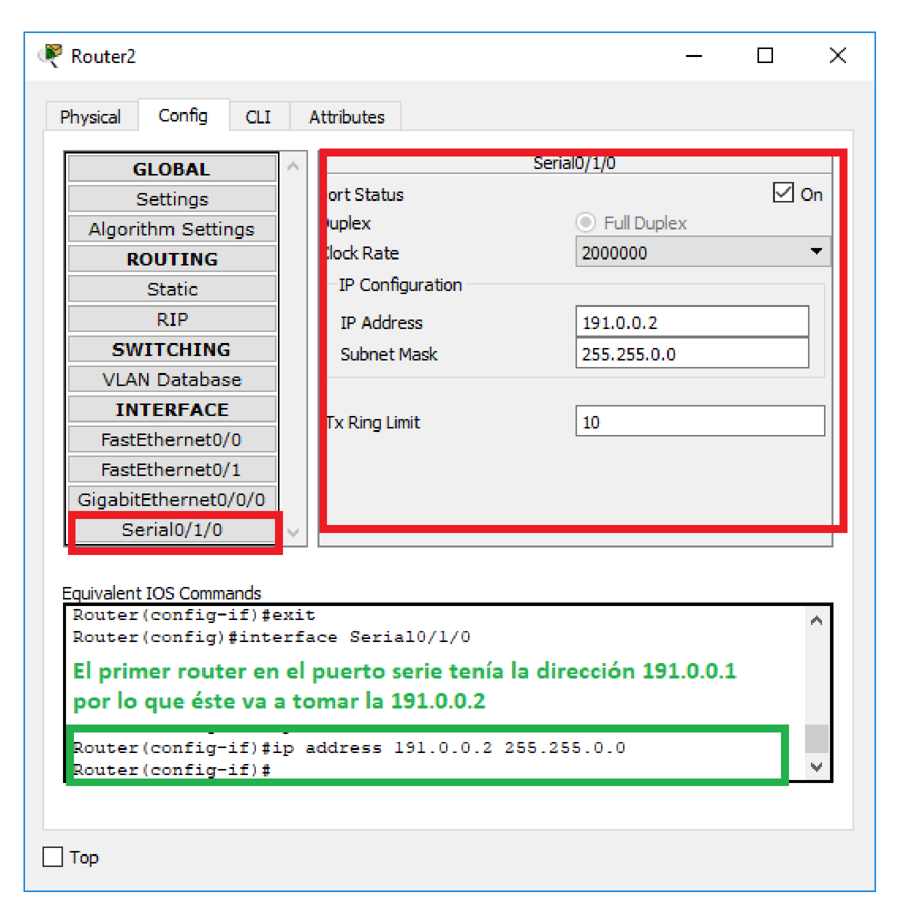

Nótese que para este paso, como se indica marcado en verde, los comandos equivalentes serían:

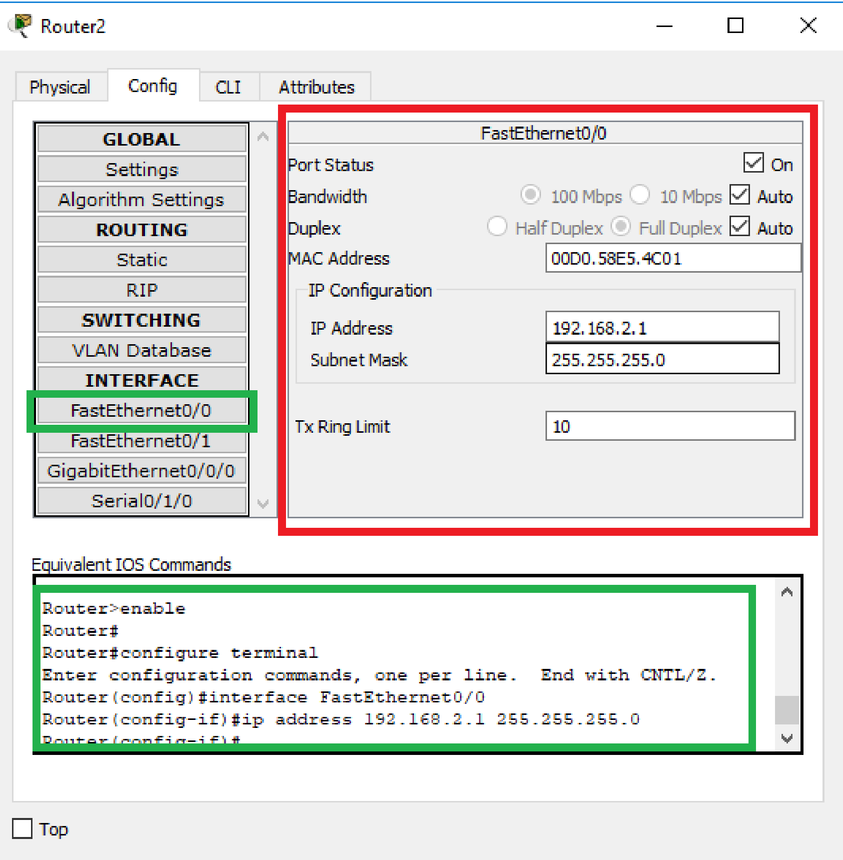
```
interface Serial0/0/0

ip address 191.0.0.1 255.255.0.0

no shutdown
```

Ahora, para terminar la configuración lógica, lo que está quedando pendiente es la configuración del **segundo router**, el que conectaría la segunda subred, la que se desarrolló en el apartado anterior. Básicamente la configuración del router es la misma, excepto que su interfaz de red conectada a su switch tomará la dirección 192.168.2.1 con máscara 255.255.255.0, y su puerto serial tomará la IP 191.0.0.2 con máscara 255.255.0.0, en las imágenes siguientes puede verse dicha configuración, remarcando en verde los comandos equivalentes para realizar los mismos pasos en la línea de comandos de un router CISCO real:


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
GigabitEthernet0/0/0
Serial0/1/0
Serial0/1/0
ort Status
On
uplex
Full Duplex
lock Rate
2000000
IP Configuration
IP Address
191.0.0.2
Subnet Mask
255.255.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#exit
Router(config)#interface Serial0/1/0
El primer router en el puerto serie tenía la dirección 191.0.0.1
por lo que éste va a tomar la 191.0.0.2
Router(config-if)#ip address 191.0.0.2 255.255.0.0
Router(config-if)#
Top

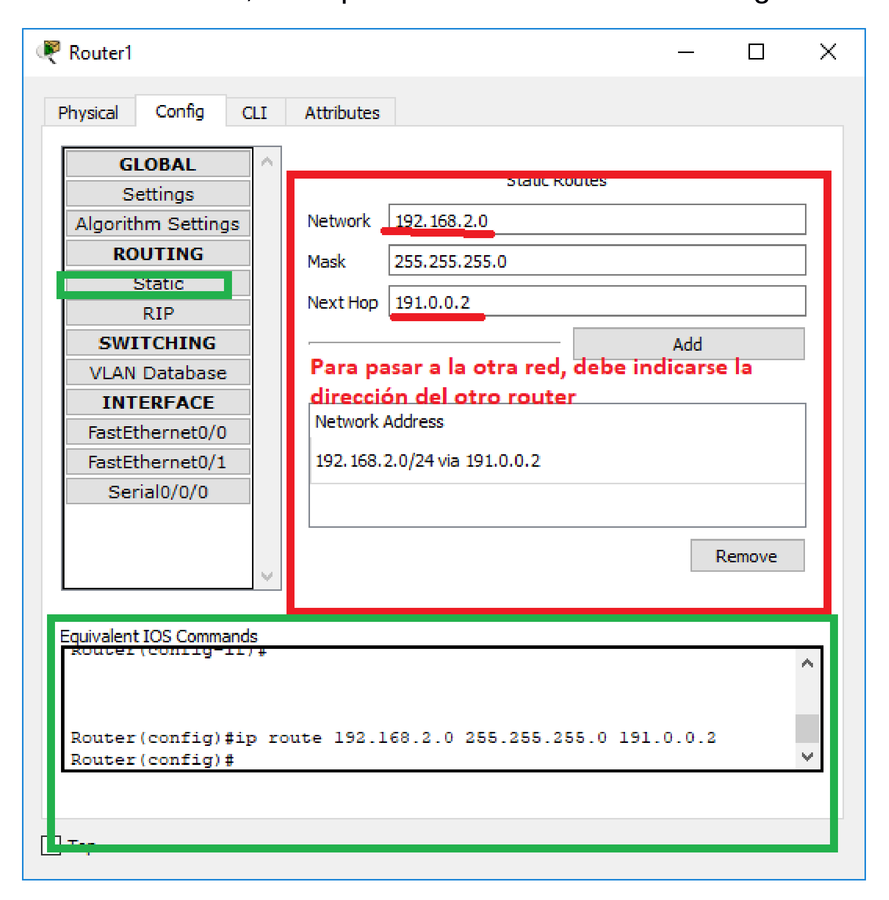

Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
GigabitEthernet0/0/0
Serial0/1/0
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.58E5.4C01
IP Configuration
IP Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Top

Realizados estos pasos, ya tenemos toda la configuración lógica de la red y de los respectivos routers, simplemente resta crear las tablas de ruteo estáticas y probar la conexión entre ambas subredes.

## Configuración de las tablas de ruteo

Para este paso, simplemente vamos a indicar a cada enrutador, por donde pasará el tráfico proveniente de la subred vecina. Es decir, añadiremos para cada red conectada (en este caso hay una sola) una tabla de ruteo que asocie a dicha red con la dirección del router que tiene conectado.

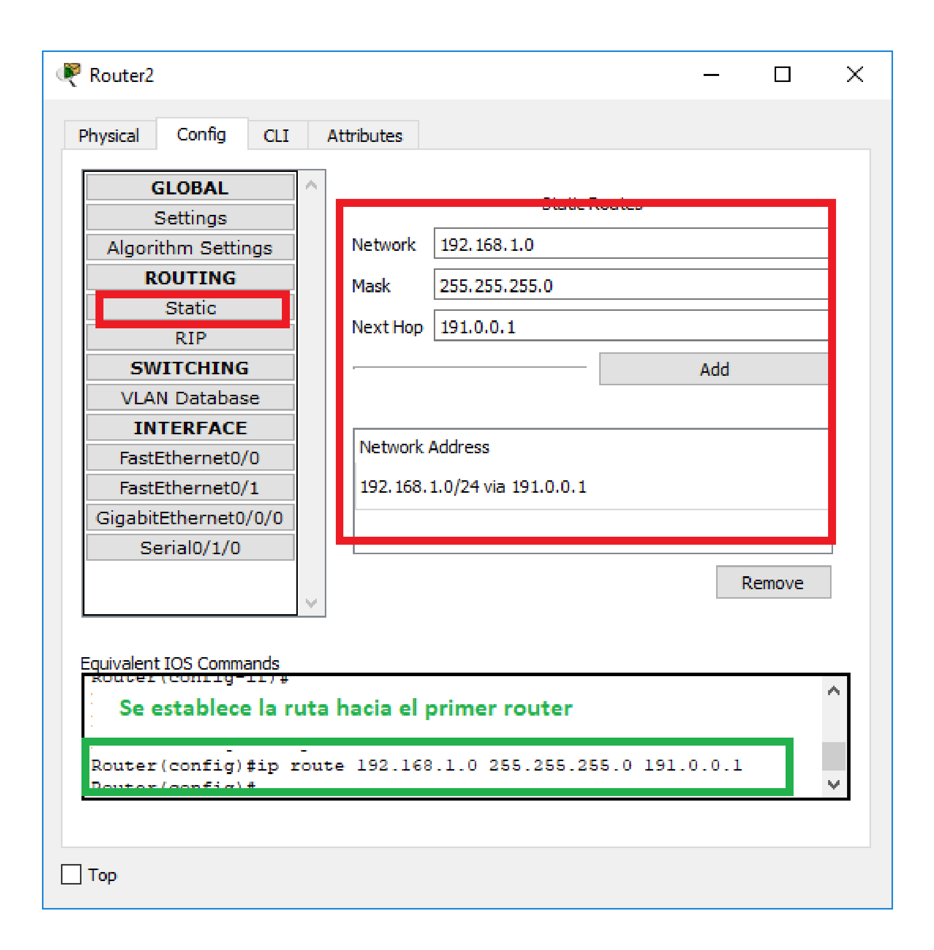
Para ello, en el primer router realizamos la siguiente configuración:



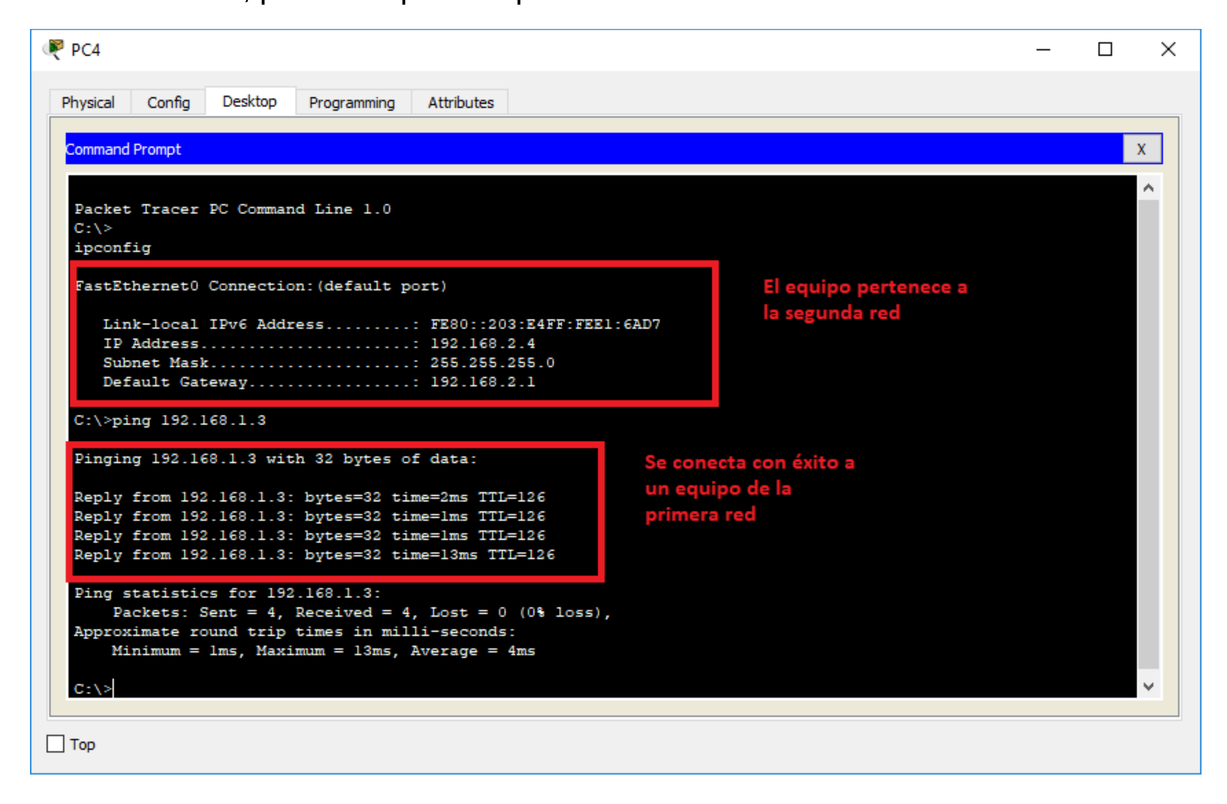

Esta directiva, lo que le está indicando al router es "para todo el tráfico que se dirija a la red de la forma 192.168.2.0, que salte al router con la dirección 192.0.0.2. Desde la línea de comandos sería el comando señalizado en verde:

```
ip route 192.168.2.0 255.255.255.0 191.0.0.2
```

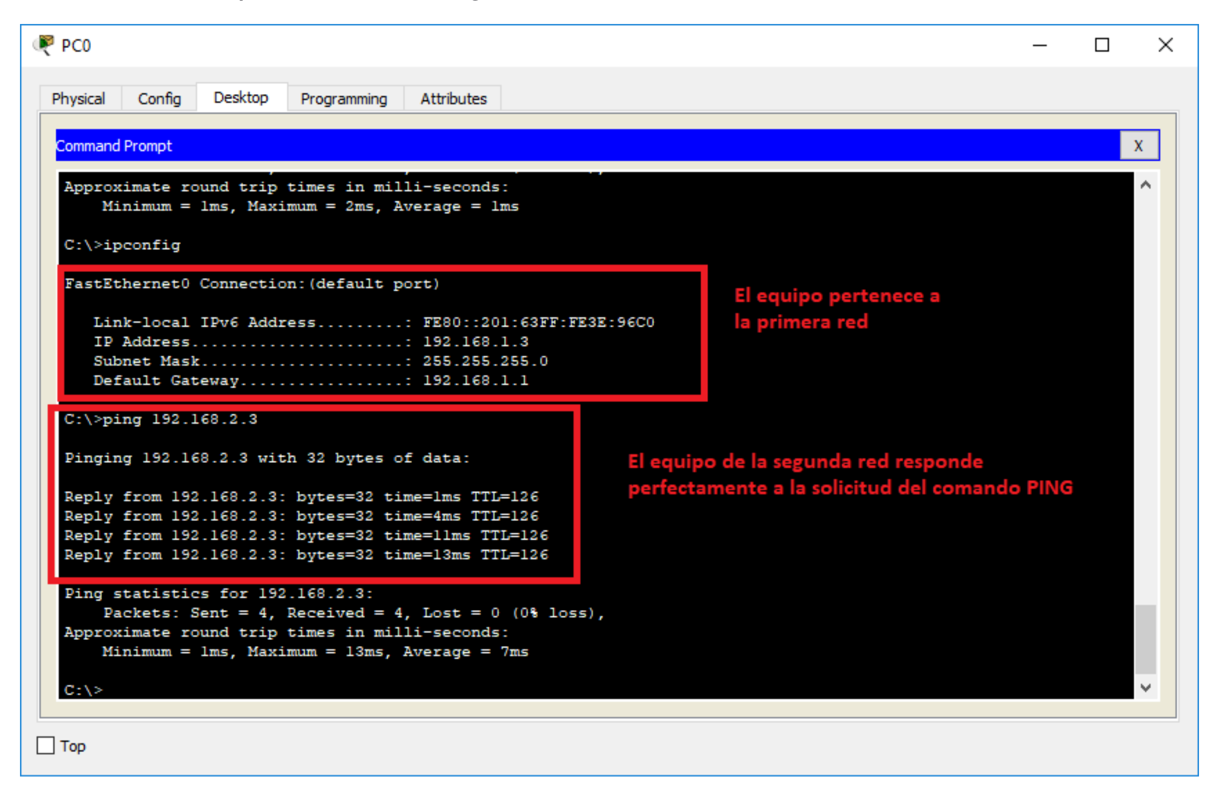
De manera análoga, al router conectado a la **segunda subred**, indicaremos que todo el tráfico que se dirija a la red con forma 192.168.1.0, salte al router con dirección 191.0.0.1:




Si hemos realizado bien los pasos anteriores y hemos configurado correctamente nuestras redes, podemos pasar a probar conexión desde una subred hacia otra:



En el ejemplo anterior probamos enviar una solicitud desde un equipo de la segunda subred hacia otro equipo con una dirección correspondiente a la primera, ahora si nos posicionamos sobre el primer equipo de la primera subred, y queremos conectarnos al primero de la segunda, obtenemos el mismo resultado:




## Capa de Transporte

La capa cuatro o capa de transporte es la encargada de asegurar que los paquetes de datos lleguen en secuencia y sin errores desde un equipo transmisor a un receptor, intercambia la información de la recepción de los datos y se encarga de retransmitir los paquetes perdidos.

Brinda comunicación lógica **entre procesos** de aplicación que se ejecutan en terminales o hosts diferentes, estableciendo la comunicación que se conoce como **punto a punto.**

**Desde el lado del transmisor** genera los segmentos a partir de los mensajes de aplicación (esto es, desde las capas superiores, que provienen desde la interacción con el usuario final hasta los procesos generados por las aplicaciones) y los transfiere a la capa de red.

**Desde el lado del receptor,** a partir de los segmentos, los mensajes se transfieren a las capas superiores. La definición y composición de los segmentos, va a depender del protocolo a utilizar en capa de transporte, los cuales pueden ser el Protocolo de Control de Transmisión (TCP), el Protocolo de Datagramas de Usuario (UDP) y el Protocolo de Transmisión para el Control de Flujo (SCTP). Los protocolos TCP y SCTP proporcionan

un servicio completo y fiable; UDP proporciona un servicio de datagramas que es rápido, pero poco fiable.

Para entender los contenidos a desarrollar sobre los servicios brindados por la capa de transporte, es importante que el lector comprenda lo que se trató en una unidad anterior sobre Servicios orientados a Conexión y Servicios sin conexión.

## Protocolo de Control de Transmisión (TCP)

*TCP (Protocolo de Control de Transmisión, del inglés Transmission Control Protocol) se diseñó específicamente para proporcionar un flujo de bytes confiable de extremo a extremo a través de una interred no confiable. Una interred difiere de una sola red debido a que sus diversas partes podrían tener diferentes topologías, anchos de banda, retardos, tamaños de paquete y otros parámetros. TCP se diseñó para adaptarse de manera dinámica a las propiedades de la interred y sobreponerse a muchos tipos de fallas.*

(Tanembaum, 2014)

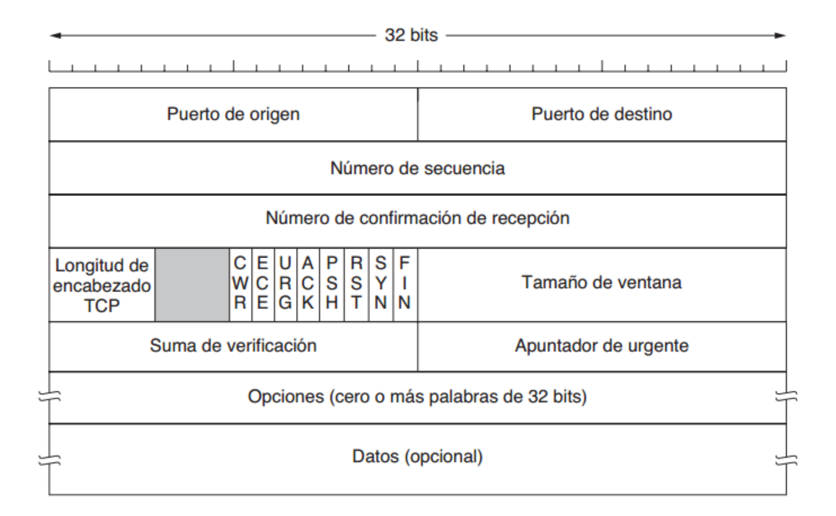
El servicio TCP se obtiene de que tanto el emisor de la información (que a nivel de comunicación actúa como servidor) y el receptor (cliente) establezcan puntos terminales llamados **sockets**, los sockets (del Inglés, “enchufes”) tienen un número de dirección que es la dirección IP del host y un número de 16 bits que es conocido como **puerto**. Un puerto es una interfaz para comunicarse con un programa a través de una red, y si bien, podría llegar a ser usado cualquier puerto para cualquier protocolo, la entidad IANA los ha normalizado y clasificado en categorías; TCP utiliza por convención los puertos 23, 25 y 53.

### Segmentos TCP

TCP se ocupa de convertir el flujo de datos saliente de una aplicación de forma que se pueda entregar como fragmentos. La aplicación traslada los datos a TCP y éste sitúa los datos en un buffer de envío. TCP toma un trozo de esos datos y le añade una una cabecera para conformar el segmento. Este segmento es trasladado a la capa de red para que lo entregue como un datagrama. El empaquetado de estos datos en trozos de tamaño adecuado permite usar de una manera eficiente los servicios de transmisión.

En los encabezados TCP, los números de secuencia y de confirmación de recepción se manejan contando bytes de datos (no segmentos) y lo que se conoce como “tamaño de la ventana” es el número de bytes que el receptor está dispuesto a recibir.

En la siguiente imagen, se puede observar la composición de un encabezado TCP:




(Imagen obtenida del libro “Redes de Computadores”, de Tanembaum)

## Funcionamiento del protocolo TCP

Existen algunos aspectos generales a considerar antes de profundizar en cómo funciona una conexión TCP, para empezar que es una conexión **punto a punto**, esto es, que tiene exactamente dos puntos terminales, no soporta la difusión ni la multidifusión. La conexión es **full dúplex**, esto quiere decir que el tráfico puede ir en ambas direcciones al mismo tiempo, y que una conexión de este tipo es un **flujo de bytes**, no un flujo de mensajes, los límites de los mensajes no se preservan de un extremo al otro, la forma en la que los mensajes son fragmentados y entregados al receptor son transparentes a éste.

Es un protocolo **orientado a conexión**, lo que implica que utiliza metodologías de “handshaking” (del inglés, “Apreton de manos”) que quiere decir que se intercambian mensajes de control, para asegurar la autenticidad e identificación de las partes. Maneja un **flujo controlado**, esto es, que posee procedimientos para evitar que un emisor rápido inunde de información y sature un receptor más lento.

Las conexiones TCP se componen de tres etapas fundamentales:

- Establecimiento de la conexión
- Transferencia de Datos
- Fin de la conexión

### Establecimiento de la conexión

El establecimiento de la conexión es un método de triple handshaking, esto es, negociación en tres pasos, ahora veremos por qué.

Aunque es posible que un par de entidades finales comiencen una conexión entre ellas simultáneamente, normalmente una de ellas abre un socket en un determinado puerto TCP y se queda a la escucha de nuevas conexiones. Es común referirse a esto como apertura pasiva, y determina el lado servidor de una conexión. El lado cliente de una conexión realiza una apertura activa de un puerto enviando un paquete **SYN**(un bit de control) inicial al servidor como parte de la negociación en tres pasos. En el lado del servidor (este receptor también puede ser una PC o alguna estación terminal) se comprueba si el puerto está abierto, es decir, si existe algún proceso escuchando en ese

puerto, pues se debe verificar que el dispositivo de destino tenga este servicio activo y esté aceptando peticiones en el número de puerto que el cliente intenta usar para la sesión. En caso de no estarlo, se envía al cliente un paquete de respuesta con el bit **RST** activado (El bit RST es un bit que se encuentra en el campo del código en el protocolo TCP y se utiliza para reiniciar la conexión.), lo que significa el rechazo del intento de conexión.

En caso de que sí se encuentre abierto el puerto, el lado servidor respondería a la petición SYN válida con un paquete SYN/ACK. Finalmente, el cliente debería responderle al servidor con un **ACK** (del inglés "*acknowledgement"* –asentimiento-, es un mensaje que el destino de la comunicación envía al origen de esta para confirmar la recepción de un mensaje) completando así la negociación en tres pasos (SYN, SYN/ACK y ACK) y la fase de establecimiento de conexión. Es interesante notar que existe un número de secuencia generado por cada lado, ayudando de este modo a que no se puedan establecer conexiones falseadas.

En la siguiente imagen se representa este procedimiento de triple handshaking:

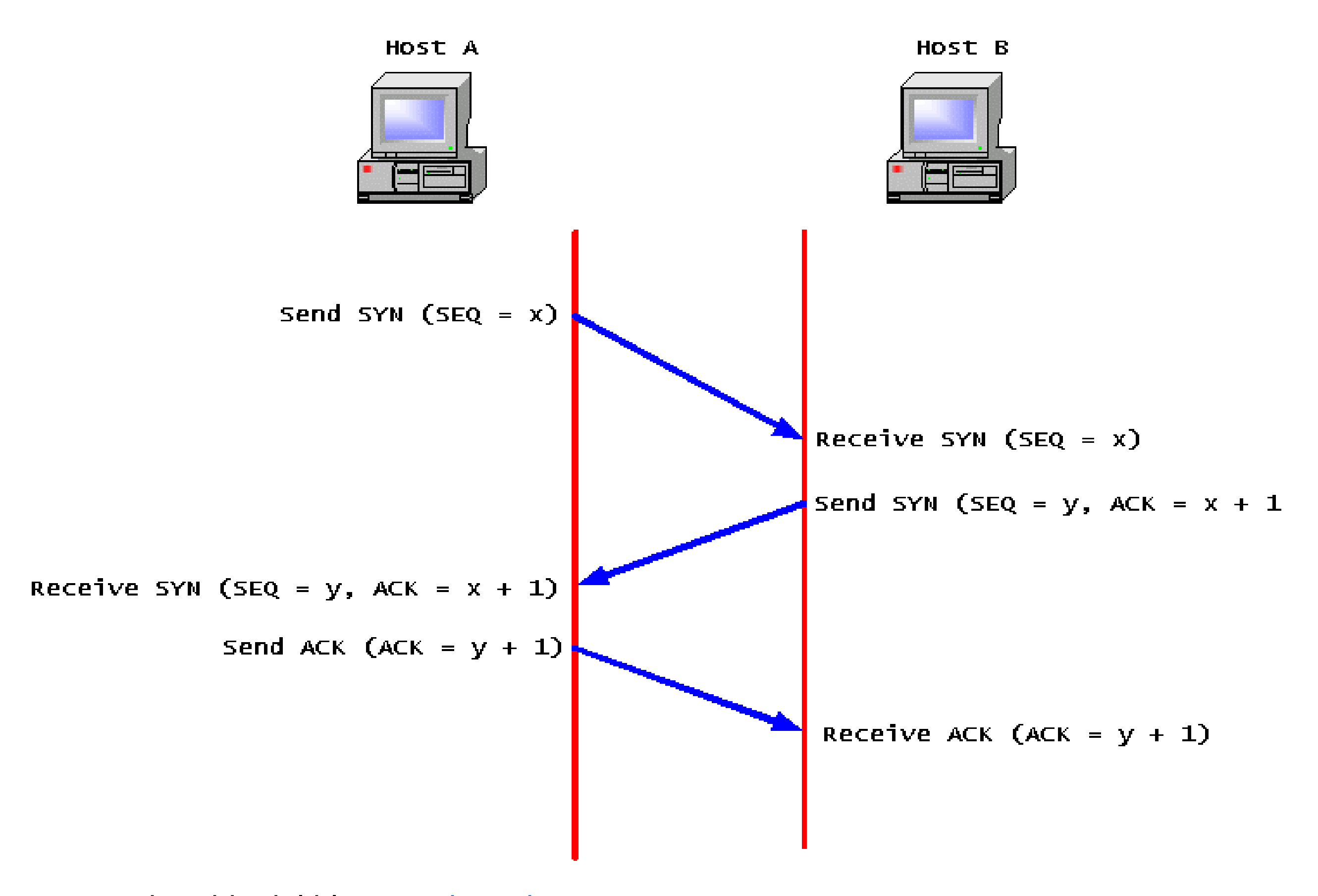



Imagen obtenida del blog Javainterview

Transferencia de datos

El segundo paso importante del mecanismo de TCP para poder establecer la comunicación, es la transferencia de datos propiamente dicha, una vez que la conexión se ha establecido.

Para garantizar la integridad de la información, TCP emplea varios mecanismos que lo convierten en un sistema muy robusto, Entre ellos están incluidos el uso del **número de secuencia** para ordenar los segmentos TCP recibidos (ya que puede ocurrir que el destinatario no los reciba en orden) y detectar paquetes duplicados, ***checksums*** para detectar errores , asentimientos y temporizadores para detectar pérdidas o retrasos y **ventanas deslizantes** para el control de flujo de datos. La ventana deslizante es un dispositivo de control de flujo que funciona por software, es decir, el control del flujo se lleva a cabo mediante el intercambio específico de caracteres o tramas de control, con los que el receptor indica al emisor cuál es su estado de disponibilidad para recibir datos (este tipo de mecanismos es lo que evita la inundación de un receptor más lento).

Finalización de la Conexión

Para esta etapa, TCP utiliza mecanismos de control al igual que para establecer la conexión, con la diferencia de que se realiza negociación de cuatro vías o “four way handshake”, empleando la transferencia de paquetes FIN entre ambas partes. Los paquetes FIN son paquetes que la única función que cumplen es notificar al equipo interlocutor que ya se ha finalizado la transferencia de datos, y que el anterior paquete enviado era el último.

*Cuando uno de los dos extremos de la conexión desea parar su "mitad" de conexión transmite un segmento con el flag FIN en 1, que el otro interlocutor asentirá con un ACK. Por tanto, una desconexión típica requiere un par de segmentos FIN y ACK desde cada lado de la conexión.*

*Una conexión puede estar "medio abierta" en el caso de que uno de los lados la finalice pero el otro no. El lado que ha dado por finalizada la conexión no puede enviar más datos pero la otra parte si podrá.*

En la imagen siguiente, pude ilustrarse este procedimiento:

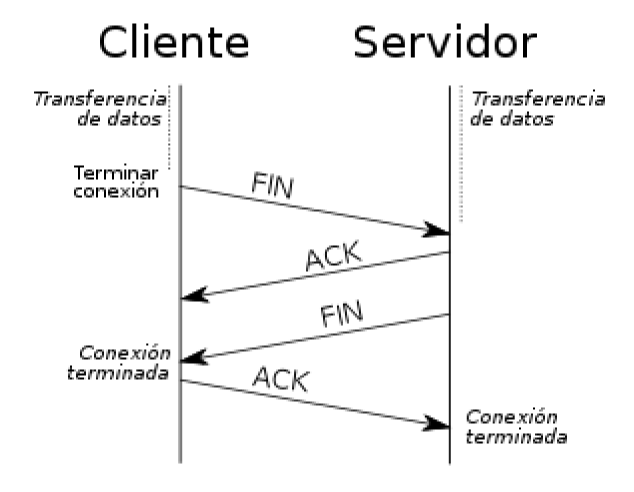



*Imagen e información marcada extraídas de Wikipedia*

## Protocolo de Datagramas de Usuario (UDP)

*UDP proporciona una forma para que las aplicaciones envíen datagramas IP encapsulados sin tener que establecer una conexión. El protocolo UDP se describe en el RFC 768. UDP transmite **segmentos** que consisten en un encabezado de 8 bytes seguido de la carga útil. En la figura 6-27 se muestra ese encabezado. Los dos **puertos** sirven para identificar los puntos terminales dentro de las máquinas de origen y destino. Cuando llega un paquete UDP, su carga útil se entrega al proceso que está conectado al puerto de destino. Este enlace ocurre cuando se utiliza la primitiva BIND o algo similar (…) el valor principal de contar con UDP en lugar de simplemente utilizar IP puro es la adición de los puertos de origen y destino. Sin los campos de puerto, la capa de transporte no sabría qué hacer con cada paquete entrante. Con ellos, entrega el segmento incrustado a la aplicación correcta.*

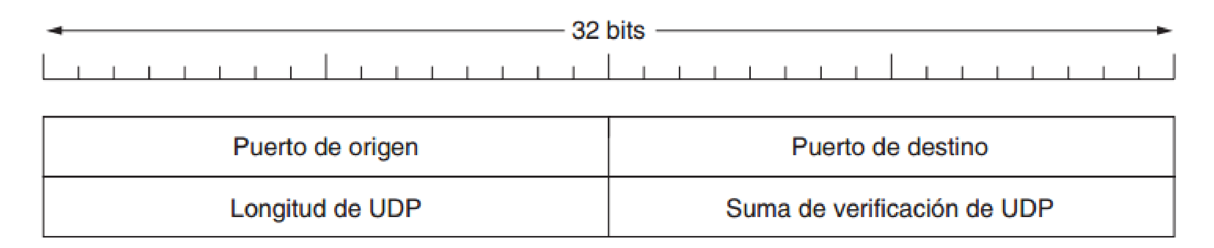



**Figura 6-27.** El encabezado UDP.

*Información marcada e imagen obtenidas del libro "Redes de Computadoras", Tanembaum, 2014.*

Este protocolo se basa en el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos en los que el intercambio de paquetes de conexión y desconexión son mayores que en TCP, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos. Un ejemplo de protocolo que utiliza UDP es el ya trabajado DHCP.

### Comparativa con TCP

Como ya se ha mencionado, UDP es un protocolo donde la transmisión de datos es mucho más simple y **no es orientado a conexión**, es decir, es mucho más insegura también, sin embargo es preferible utilizar UDP cuando el flujo de bits es demasiado grande para establecer parámetros previos de autentificación y garantización de la integridad de los datos, como se decía más arriba, el caso de la retransmisión de audio y de video.

TCP es preferible cuando la integridad de la información es imprescindible, además de ser más sencillo de implementar a nivel de programación. Si se está desarrollando una

aplicación con comunicación cliente/servidor, los mecanismos para control de flujo, chequeo de la integridad de los datos mediante suma de comprobación, o de control son completamente transparentes al programador, y son manejados por funciones primitivas del protocolo, si se opta por UDP para poder tener mayor velocidad y transferir grandes cantidades de información pero a su vez se quiere garantizar mayor robustez a la transferencia, entonces el programador deberá desarrollar por su cuenta los procedimientos para este fin.

### Implementación en lenguajes de programación

Si bien no es propósito de esta guía tratar los protocolos con tanta profundidad como para llegar a la implementación en un lenguaje de programación, además de que ya se estaría ingresando demasiado en el campo de otra disciplina informática, se sugiere al lector que necesite implementar alguno de estos protocolos, la lectura de artículos con dicho contenido.

Existe una amplia bibliografía de Programación referida a esto, pero como en esta guía siempre se apuesta a la información de libre y fácil acceso, se sugiere la lectura de los siguientes artículos:

- Para la implementación de UDP en Gambas3, Java, Python y C, se recomienda la lectura del artículo de UDP de Wikipedia en donde se citan los algoritmos.
- Para la implementación tanto de TCP como de UDP específicamente utilizando el lenguaje Java, se recomienda la lectura sobre sockets en Java que se encuentra en Programación.com.py
- Para la implementación en cualquier otro lenguaje de programación, o la búsqueda de cualquier otro ejemplo, se invita al lector a buscar esto por sus propios medios.

# Capa de Aplicación

Seguramente si hemos pasado de la capa de transporte a la de aplicación, usted lector interpretará que esta guía está basada en el protocolo TCP/IP y no en el modelo OSI, o también dado a la manera de expresar cada capa quizás interprete que nos estamos basando en el modelo OSI pero nos olvidamos de las capas de sesión y aplicación, y esto no es tan así, en ningún caso.

Tanto el modelo TCP/IP como el modelo OSI son modelos de referencia válidos para explicar arquitectura de redes y los diferentes niveles intervinientes en la comunicación. En general, el modelo TCP/IP posee una pila de protocolos ampliamente utilizada, aunque el esquema en sí, presenta varias dificultades (para empezar porque carece de una capa física), el modelo OSI por su parte, posee protocolos que ya están obsoletos y casi no se utilizan, pero es un modelo de referencia que explica con claridad una división en capas de un esquema que sigue siendo válido, por esta razón, se han trabajado protocolos actuales desde una perspectiva teórica o conceptual que responde al modelo de referencia OSI.

De todas maneras, el propósito general de esta guía es brindar una introducción a las redes de computadoras de tal modo que para aquel lector que tenga muy poco o ningún conocimiento del tema, logre una abstracción global de su funcionamiento y los diferentes niveles existentes, así como también de los diferentes dispositivos que intervienen en el ensamblado de las redes, conociendo los procedimientos prácticos para crear redes de pequeño alcance, y los conceptos globales que conciernen a las redes de amplio alcance. Dicho esto, parece importante detallar y trabajar con protocolos de capas en las cuales se realiza mayor cantidad de configuraciones, y son de amplio renombre a la hora de trabajar con redes.

Como la capa de sesión es transparente no sólo al usuario sino también al desarrollador de aplicaciones, incluso al administrador de redes cuando trabajamos a nivel general, en las tareas de mantenimiento de redes domésticas, y es encargada de mantener abierta la sesión o la conversación a nivel de servicios del sistema, es que no está en nuestro cometido profundizar en ella ahora.

Por otro lado, la capa de presentación es la responsable de que las aplicaciones de usuario puedan “entender” la información proveniente de capas inferiores. Es decir, se encarga del formato de los datos. Cuando enviamos un correo electrónico, por ejemplo, la aplicación que utilice el usuario va a manipular diferentes tipos de datos de diferente naturaleza (textos, archivos multimedia, etc) que para que sean transferidos a capas inferiores deben ser formateados de tal modo que pueda ser tratada por los protocolos correspondientes e interpretada por el nivel de aplicación de forma transparente al usuario de destino. Tampoco vamos a realizar configuraciones ni profundizar en los protocolos de esta capa, por lo que daremos paso al estudio de la última capa, la capa de Aplicación, la séptima del modelo OSI o la cuarta en el modelo TCP/IP, ya que es la que tiene interacción directa con las aplicaciones de las que hace uso el usuario final, y por lo tanto, resulta importante conocer el funcionamiento de algunos de sus protocolos.

## Funciones de la capa de Aplicación

Ofrece a las aplicaciones (las que pueden ser de usuario o de sistema), la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y protocolos de transferencia de archivos.

Un punto que se debe aclarar ante todo, es que el usuario no interactúa en forma directa con el nivel de aplicación, sino que interactúa con los programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

Así por ejemplo un usuario no manda una petición para obtener el fichero "index.html" para acceder a la página principal de un sitio web, ni tiene por qué leer directamente el código HTML si lo que quiere es visitar el sitio sin interesarse por su construcción interna. Cuando se utiliza una aplicación de mensajería, no es necesario que codifiquemos la información y los datos del destinatario para entregarla a la capa de Presentación y así para que ésta realice el envío del paquete. De lo anterior, se debe tener presente que **la capa de aplicación se encarga de ofrecer a las aplicaciones el acceso a la red transfiriendo información hacia las demás capas, utilizando protocolos específicos de aplicación para la comunicación con dichas aplicaciones.**

*En esta capa aparecen diferentes protocolos y servicios:*

*Protocolos:*

- *FTP (File Transfer Protocol - Protocolo de transferencia de archivos) para transferencia de archivos.*
- *DNS (Domain Name System - Sistema de nombres de dominio).*
- *DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de anfitrión).*
- *HTTP (HyperText Transfer Protocol) para acceso a páginas web.*
- *HTTPS (Hypertext Transfer Protocol Secure) Protocolo seguro de transferencia de hipertexto.*
- *POP (Post Office Protocol) para recuperación de correo electrónico.*
- *SMTP (Simple Mail Transport Protocol) para envío de correo electrónico.*
- *SSH (Secure SHell)*
- *TELNET para acceder a equipos remotos.*
- *TFTP (Trivial File Transfer Protocol).*
- *LDAP (Lightweight Directory Access Protocol).*
- *XMPP, (Extensible Messaging and Presence Protocol) - Protocolo estándar para mensajería instantánea.*

*Servicios:*

- *Aplicaciones de Red*
- *www (World Wide Web).*
- *enlace a capas inferiores*

*Esta capa contiene las aplicaciones visibles para el usuario. Algunas consideraciones son: seguridad y cifrado, DNS (Domain Name Service) Una de las aplicaciones más usadas hoy en día en Internet es el WWW (World Wide Web).*

*Información obtenida de Wikipedia*

## Algunos protocolos de Aplicación

Ahora entraremos un poco en detalle con algunos protocolos que se han citado anteriormente pero que a demás son tan conocidos que todo aquel lector que se haya capacitado en esta u otras áreas de la Informática, o que se encuentre familiarizado al lenguaje informático, seguramente habrá escuchado nombrar o incluso tal vez ya previamente conozca.

### DNS: Sistema de Nombres de Dominio

Del Inglés "Domain Name System" es un sistema de nomenclatura jerárquico que permite a dispositivos conectados a redes que funcionan bajo el protocolo IP, como redes privadas, domésticas o la misma Internet; asociar una dirección IP con un nombre de dominio.

El sistema asocia información variada de un participante de la red a un nombre de dominio que lo identifica de manera única.

Los servidores DNS utilizan una base de datos distribuida y jerárquica que almacena información asociada a cada nombre de dominio en la red, en Internet es de vital importancia ya que facilita el uso de la World Wide Web a usuarios finales totalmente ajenos a la informática, y en definitiva a cualquier usuario de un sitio web que puede asociar al sitio con nombres amigables y fáciles de recordar, analicemos la siguiente reflexión:

*Aunque en teoría los programas pueden hacer referencia a páginas web, buzones de correo y otros recursos mediante las direcciones de red (por ejemplo, IP) de las computadoras en las que se almacenan, a las personas se les dificulta recordar estas direcciones. Además, navegar en las páginas web de una empresa desde un servidor con la dirección 128.111.24.41 significa que si la compañía mueve el servidor web a una máquina diferente con una dirección IP distinta, hay que avisar a todos sobre la nueva dirección IP. Por este motivo se introdujeron nombres legibles de alto nivel con el fin de separar los nombres de máquina de las direcciones de máquina. De esta manera, el servidor web de la empresa podría conocerse como www.cs.washington.edu sin importar cuál sea su dirección IP. Sin embargo, como la red sólo comprende*

*direcciones numéricas, se requiere algún mecanismo para convertir los nombres en direcciones de red.*

(Tanembaum, 2014)´

En la siguiente imagen, se muestra una tabla con una lista de dominios genéricos de nivel superior, es decir, no son dominios necesariamente asociados a ningún país en específico, también se especifica si se trata de dominios restringidos o si por el contrario, cualquier persona puede reservarlos para su sitio web:

| Dominio | Uso deseado | Fecha de inicio | ¿Restringido? |
|---|---|---|---|
| com | Comercial | 1985 | No |
| edu | Instituciones educativas | 1985 | Sí |
| gov | Gobierno | 1985 | Sí |
| int | Organizaciones internacionales | 1988 | Sí |
| mil | Milicia | 1985 | Sí |
| net | Proveedores de red | 1985 | No |
| org | Organizaciones sin fines de lucro | 1985 | No |
| aero | Transporte aéreo | 2001 | Sí |
| biz | Negocios | 2001 | No |
| coop | Cooperativas | 2001 | Sí |
| info | Informacional | 2002 | No |
| museum | Museos | 2002 | Sí |
| name | Personas | 2002 | No |
| pro | Profesionales | 2002 | Sí |
| cat | Catalán | 2005 | Sí |
| jobs | Empleo | 2005 | Sí |
| mobi | Dispositivos móviles | 2005 | Sí |
| tel | Detalles de contacto | 2005 | Sí |
| travel | Industria de viajes | 2005 | Sí |
| xxx | Industria del sexo | 2010 | No |

*Imagen tomada del libro "Redes de Computadoras" de Tanembaum, 204*

El sistema DNS utiliza el puerto 53 tanto para TCP como para UDP.

## Protocolo de Transferencia de Hipertexto (HTTP)

*El **Protocolo de transferencia de hipertexto** (en inglés: **Hypertext Transfer Protocol** o **HTTP**) es el protocolo de comunicación que permite las transferencias de información en la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. HTTP es un protocolo sin estado, es decir, no guarda ninguna información sobre conexiones*

*anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de sesión, y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.*

*Información obtenida de [Wikipedia]*

Cabe destacar, que actualmente el protocolo HTTP se encuentra en la versión 2.0, y que opera con el puerto de comunicaciones número 80. HTTPS es una variante de éste protocolo, que se define como seguro, pues además de brindar la funcionalidad expresada en HTTP, encripta la información sensible (generalmente nombres de usuario y contraseñas) que viaja a través de la web entre el servidor y el navegador del usuario, para asegurar mayor confidencialidad de los datos, para el cifrado utiliza SSL o TLS. HTTPS hace uso del puerto 443.

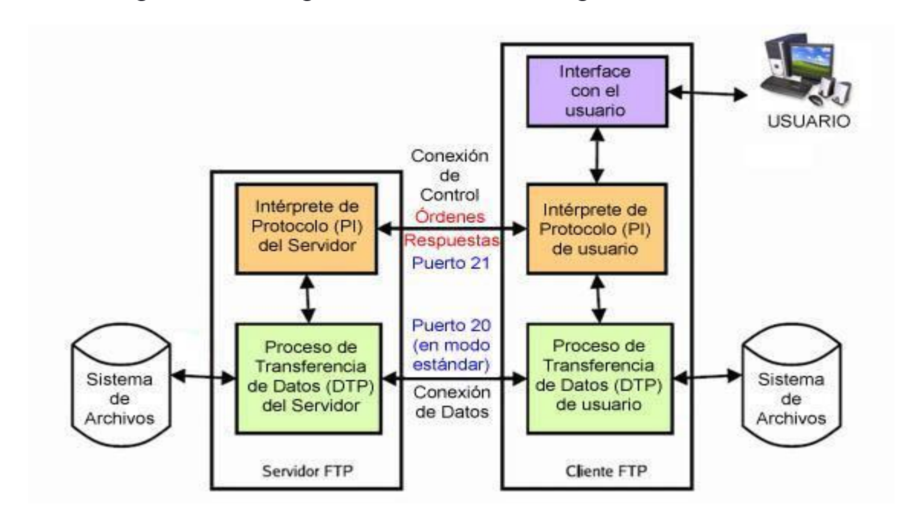
## Protocolo de Transferencia de Archivos (FTP)

*El **Protocolo de transferencia de archivos** (en inglés **File Transfer Protocol** o **FTP**), es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.*

*El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.*

*Para solucionar este problema son de gran utilidad aplicaciones como SCP y SFTP, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico.*

En la siguiente imagen se ilustra el diagrama de un servicio FTP:




*Información marcada e imagen obtenida de Wikipedia*

## Protocolo de Configuración Dinámica del Host (DHCP)

Se trabajó anteriormente en el apartado de Capa de Red, ya que es un protocolo que trabaja sobre IP, y es esencial para la configuración de redes manejando parámetros que tienen que ver directamente con este último. No obstante, teniendo en cuenta el servicio ofrecido a las aplicaciones, que no requieran configurarse bajo direcciones fijas cuando trabajan a nivel cliente / servidor, DHCP es considerado un protocolo de Aplicación, para profundizar en él, se sugiere volver a Servicio DHCP.

## Intérprete de Órdenes Seguro (SSH)

**El significado del protocolo es Secure Shell (**en español: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a servidores a través de lo que se conoce como una puerta trasera (también conocida *backdoor*). Permite manejar por completo el servidor mediante un intérprete de comandos, y también puede redirigir el tráfico de X (En sistema de Ventanas X, donde se podía dotar de interfaz gráfica a sistemas Unix) para poder ejecutar programas gráficos si tenemos ejecutando un Servidor X (soportado en sistemas Unix y Windows).

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto archivos sueltos como la simulación de sesiones FTP), gestionar claves cifradas con algoritmo RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro que es tunelizado por el servicio SSH.

De lo anterior, se sobreentiende que, en un servidor debemos tener bien aseguradas las claves de acceso si tenemos habilitado para el mismo, el puerto 22 que es el utilizado por SSH, ya que si un usuario malintencionado conoce un usuario y clave autorizados, podría tener acceso total al servidor mediante SSH.

Para conocer los comandos básicos de SSH, se sugiere investigar en el siguiente artículo de la Wiki de Debian.

# Actividades prácticas extra

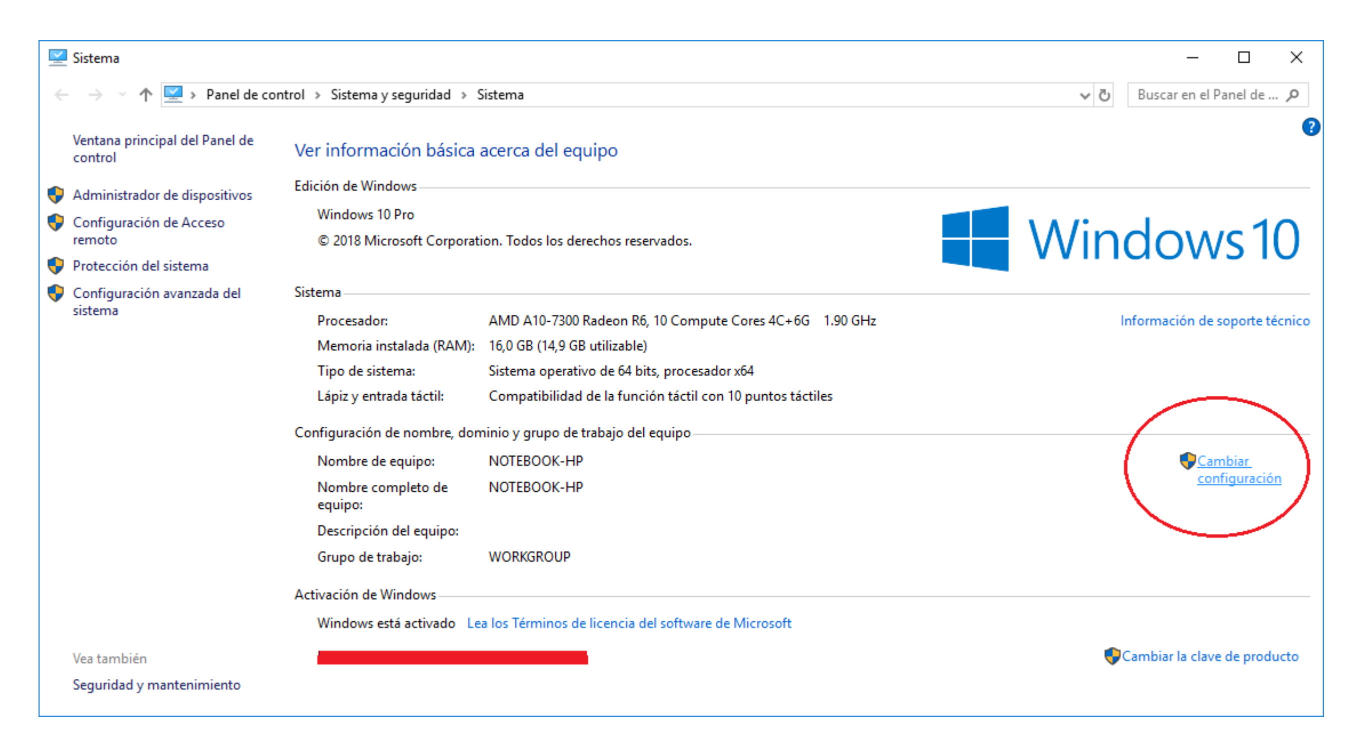
Teniendo en cuenta que ya se han trabajado los fundamentos básicos para comprender a nivel global qué es una red de computadoras, qué diferentes tipos de redes existen, dejando en claro algunos conceptos clave y habiendo pasado por prácticas como la de el armado de un cable par trenzado, el de la conexión física entre equipos armando pequeñas LAN, incluso habiendo trabajado de forma emulada por software aspectos de enrutamiento y su configuración, se considera que es interesante que cualquier lector que esté interesado en esta temática, si es que ya no está familiarizado con su aplicación práctica, sea capaz de llevar a cabo algunos procedimientos útiles, como ser el de compartir carpetas y recursos en una red local, acceder a un equipo y utilizarlo mediante SSH, o transferir archivos utilizando FTP. De modo que dedicaremos un poco al abordaje de estos temas.

## Compartir archivos e impresoras en red

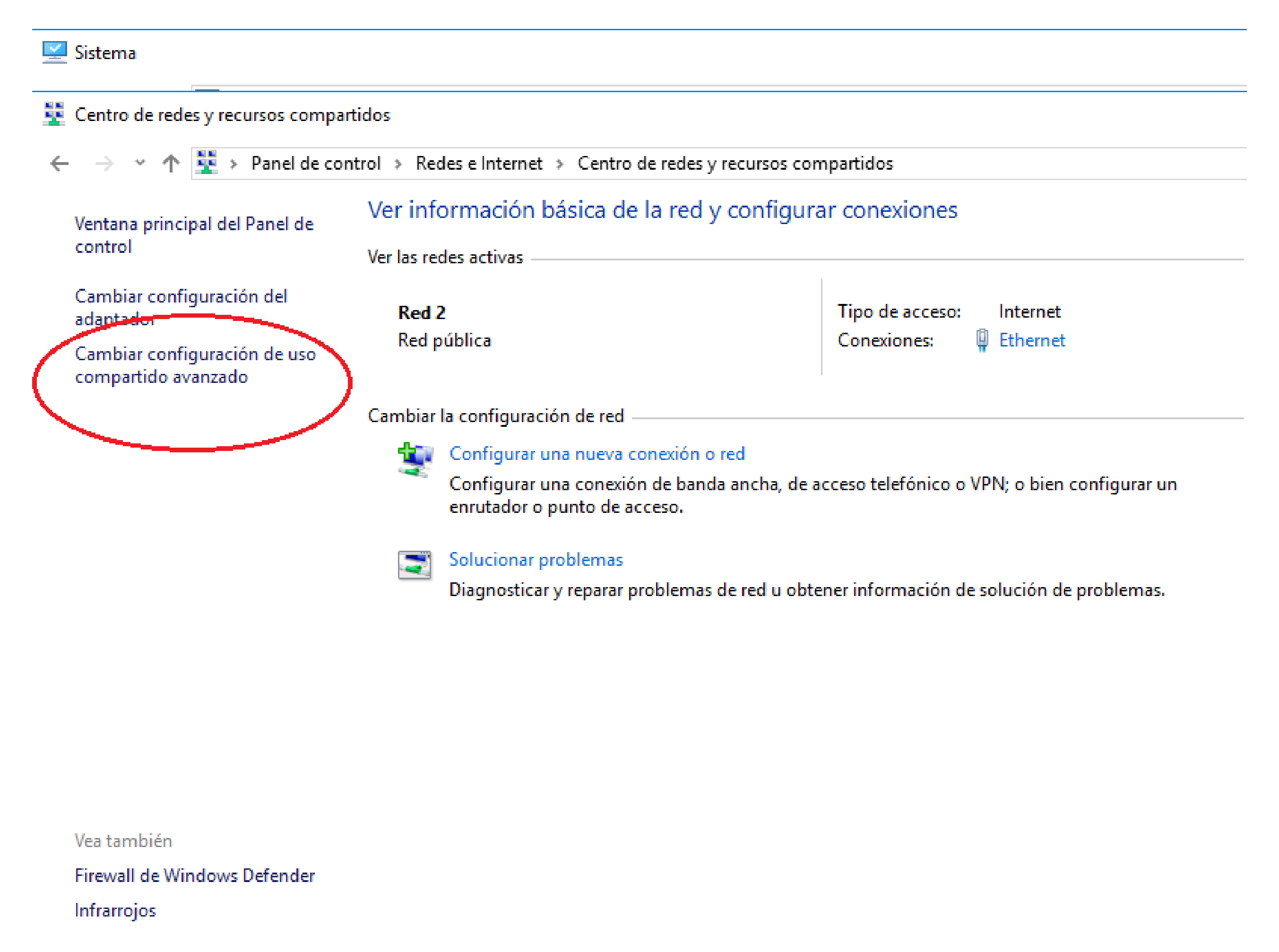
En primer lugar, para poder compartir recursos en una red es importante que dicha red exista a nivel físico, y los equipos se encuentren conectados ya sea por la vía inalámbrica o por la vía cableada a través de un switch. En todos los casos, es necesario que los equipos cuenten con direcciones de IP que pertenezcan a la misma subred, las cuales pueden ser asignadas manualmente o con un dispositivo que ofrezca servicio DHCP, esos temas ya fueron abordados anteriormente en Crear una pequeña red local entre dos o varios equipos.

### Compartir recursos en Windows

Si trabajamos en entornos Windows, es importante que todos los equipos pertenezcan al mismo grupo de trabajo, para ello debemos asegurarnos que en las propiedades de cada equipo, se encuentren asignados los nombres correspondientes, y que en todas las computadoras se encuentren asignadas el mismo nombre del grupo de trabajo, en este caso de ejemplo, usamos el nombre “WORKGROUP” que viene asignado por defecto en Windows 7 y Windows 10. Simplemente damos clic derecho en “Este Equipo” y luego elegimos la opción “Propiedades”; o bien, vamos a Panel de Control, luego a “Sistema y Seguridad”, y por último a “Sistema”. En la siguiente imagen pueden verse los mencionados parámetros y se señala la opción para cambiarlos, de ser necesarios:




Una vez que todas las computadoras se encuentran bajo el mismo grupo de trabajo, debemos asegurarnos de tener habilitada la detección de redes, y permitida también la opción de compartir archivos e impresoras. Para ello vamos a la ventana principal del Panel de Control, y elegimos “Redes e Internet”. En la ventana emergente, debemos abrir el Centro de Redes y Recursos Compartidos, debería mostrarnos una ventana como la siguiente, en la cual debemos seleccionar “Cambiar la Configuración de uso compartido avanzado”:




Una vez dentro de la configuración del uso compartido, debemos seleccionar según sea el caso (dependiendo si estamos en una red pública o privada) los parámetros para activar la detección de redes y activar el uso compartido de archivos e impresoras. En el caso de que queramos que un usuario de la red pueda acceder a la carpeta pública del equipo sin necesidad de autentificarse en él, también debemos desactivar el uso compartido con protección por contraseña.

A continuación, se muestra una captura de una posible configuración:

Cambiar opciones de uso compartido para distintos perfiles de red

Windows crea un perfil de red independiente para cada red que use. Puede elegir opciones específicas para cada perfil.

Privado

Invitado o público (perfil actual)

Detección de redes

Cuando se activa la detección de redes, este equipo puede ver otros equipos y dispositivos en la red y es visible para los demás equipos en la red.

◉ Activar la detección de redes
○ Desactivar la detección de redes

Compartir archivos e impresoras

Cuando se activa el uso compartido de archivos e impresoras, los usuarios de la red podrán tener acceso a los archivos e impresoras compartidos en este equipo.

◉ Activar el uso compartido de archivos e impresoras
○ Desactivar el uso compartido de archivos e impresoras

Todas las redes

Los demás equipos Windows conectados al mismo grupo de trabajo podrán ver nuestros archivos y carpetas compartidos en la carpeta pública de nuestra PC (por defecto “C:\Users\Public”).

Todos los archivos que copiemos en la carpeta pública, podrán ser accedidos por otros usuarios simplemente seleccionando nuestro equipo, desde el explorador de archivos, a través de la ventana de “Red”. Cabe destacar, que el proceso de configuración debe repetirse en todos los equipos Windows que quieran conectarse en la LAN.

## Compartir una impresora en Windows

Si tenemos una impresora instalada en un equipo, y queremos que sea accesible desde cualquier computadora que esté conectada a la red, simplemente tenemos que, una vez instalada, la impresora se encuentre compartida. Se adjunta la información presentada en la documentación de Microsoft para realizar la configuración desde el PC principal (donde está instalada la impresora) y luego en las PCs “secundarias” (las que utilizarán dicha impresora):

### *Compartir la impresora en el PC principal*

*Hay dos formas de compartir la impresora con la configuración o el Panel de Control.*

#### *Compartir la impresora con la configuración*

1. *Selecciona el botón* ***Inicio*** *y luego selecciona* ***Configuración*** *>* ***Dispositivos*** *>* ***Impresoras y escáneres****.*
2. *Elige la impresora que quieras quitar y selecciona* ***Administrar****.*
3. *Selecciona* ***Propiedades de impresora*** *y elige la pestaña* ***Uso compartido****.*
4. *En la pestaña Uso compartido, selecciona* ***Compartir esta impresora****.*
5. *Si quieres, edita el nombre del recurso compartido de la impresora. El nombre del recurso compartido se usa al conectarse a la impresora desde el PC secundario.*

### *Compartir la impresora con el Panel de Control*

1. *En el cuadro de búsqueda de la barra de tareas, escribe **panel de control** y después selecciona **Panel de control**.*
2. *En Hardware y sonido, selecciona **Ver dispositivos e impresoras**.*
3. *Selecciona y mantén presionado (o haz clic con el botón derecho) en la impresora que quieras compartir, selecciona **Propiedades de impresora** y, a continuación, elige la pestaña **Uso compartido**.*
4. *En la pestaña Uso compartido, selecciona **Compartir esta impresora**.*
5. *Si quieres, edita el nombre del recurso compartido de la impresora. Usa el nombre del recurso compartido al conectarse a la impresora desde el equipo cliente.*

## *Conectar la impresora compartida con el PC secundario*

*Hay dos formas de conectar la impresora con el PC secundario mediante la configuración o el Panel de Control.*

### *Conectar la impresora con la configuración*

1. *Selecciona el botón **Inicio** y luego selecciona **Configuración** > **Dispositivos** > **Impresoras y escáneres**.*
2. *En Agregar impresoras y escáneres, selecciona **Agregar una impresora o un escáner**.*
3. *Elige la impresora que quieras y selecciona **Agregar dispositivo**.*
4. *Si no ves la impresora que quieres, selecciona **La impresora que quiero no aparece en la lista**.*
5. *En el cuadro de diálogo Agregar impresora, selecciona **Seleccionar una impresora compartida por nombre** y, a continuación, escribe el nombre del equipo o dispositivo del PC principal y el nombre del recurso compartido de la impresora mediante uno de estos formatos:*
   - *\\nombreDeEquipo\nombreDeImpresora*
   - *http://nombreDeEquipo\nombreDeImpresora/.printer*
6. *Cuando se te pida instalar el controlador de la impresora, selecciona **Siguiente** para completar la instalación.*

*Para obtener más información acerca del nombre del equipo o del dispositivo, consulta la sección Encontrar el nombre de tu PC en este tema. De manera predeterminada, necesitas el nombre de usuario y la contraseña del PC principal para acceder a la impresora.*

### *Compartir la impresora con el Panel de Control*

1. *En el cuadro de búsqueda de la barra de tareas, escribe **panel de control** y después selecciona **Panel de control**.*
2. *En Hardware y sonido, selecciona **Ver dispositivos e impresoras** y luego, **Agregar una impresora**.*
3. *Selecciona la impresora que quieres y luego, **Siguiente**. Cuando se te pida, instala el controlador de la impresora.*

4. *Si no ves la impresora que quieres, selecciona* ***La impresora que quiero no aparece en la lista****.*
5. *En el cuadro de diálogo Agregar un dispositivo, selecciona* ***Seleccionar una impresora compartida por nombre*** *y, a continuación, escribe el nombre del equipo o dispositivo del PC principal y el nombre del recurso compartido de la impresora mediante uno de estos formatos:*
   - *\\nombreDeEquipo\nombreDeImpresora*
   - *http://nombreDeEquipo\nombreDeImpresora/.printer*
6. *Cuando se te pida instalar el controlador de la impresora, selecciona* ***Siguiente*** *para completar la instalación.*

*Para obtener más información acerca del nombre del equipo o del dispositivo, consulta la sección Encontrar el nombre de tu PC en este tema. De manera predeterminada, necesitas el nombre de usuario y la contraseña del PC principal para acceder a la impresora.*

Información extraída desde el Soporte de Microsoft

## Compartir archivos y carpetas en Linux

Linux no nos pone las cosas tan fáciles a la hora de compartir archivos y carpetas entre los equipos. Pero existe una razón por la que no tenemos un sistema tan automatizado, y es que permitir que se compartan archivos y carpetas en nuestro equipo como hacemos en Windows, implica nada menos que autorizar al sistema operativo a mantener abiertos puertos que permiten la transferencia de archivos, y esto puede conllevar a un problema importante de seguridad.

La mala noticia, es que debemos utilizar algunos comandos, la buena es que comprenderemos una vía más segura para poder compartir, y es mediante la utilización de **NFS,** el cual no es ni un protocolo ni un programa, sino todo un sistema de archivos para poder intercambiar ficheros en una red.

Además, NFS al ser un sistema de archivos, permite que podamos compartir recursos de red desde un equipo para que sean accedidos desde dispositivos Windows o Linux, simplemente dichos dispositivos deben tener instalado el software **cliente** de NFS, y el equipo desde el cual se comparten los archivos debe tener instalado el **servidor** NFS.

Para el caso de ejemplo, utilizaremos Ubuntu en un equipo que funcionará como servidor NFS, desde el cual debemos instalar el servicio NFS, ingresando por terminal el comando:

```
sudo apt-get install nfs-kernel-server
```

Una vez instalado, debemos simplemente tener bien presente el directorio de la carpeta compartida, para posteriormente dejarla disponible en la red, podemos crear una llamada “ejemplo” en nuestro escritorio simplemente tipeando:

```
mkdir /home/NOMBRE_USUARIO/Escritorio/compartida
```

Todos los archivos que guardemos en esa carpeta, serán accesibles desde los equipos que autoricemos en nuestro servidor NFS, para configurarlo, simplemente abrimos desde un editor de texto (por ejemplo, nano) el archivo /etc/exports:

```
sudo nano /etc/exports
```

Aparecen en líneas comentadas del fichero, las directivas para compartir una carpeta dependiendo de la versión de NFS a utilizar, en nuestro caso podríamos utilizar la versión 4, que es la más actual, copiando el código de ejemplo para NFSv4 y modificando el directorio por la ruta donde se encuentra nuestra carpeta compartida (/home/lapvirtual/Escritorio/compartida), vemos que antes del paréntesis donde se indican los modificadores de la configuración tenemos un asterisco (*), esto indica que compartimos la carpeta para TODOS los usuarios. También tenemos la opción de en este campo simplemente colocar la IP del equipo cliente con el cual se compartirá la carpeta:

```
lapvirtual@lapvirtual-VirtualBox: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
  GNU nano 2.5.3            Archivo: /etc/exports                      Modificado

# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_sub$
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#

/home/lapvirtual/Escritorio/compartida        *(rw,sync,fsid=0,crossmnt,no_subt$

                              [ Orden desconocida ]
^G Ver ayuda  ^O Guardar    ^W Buscar     ^K Cortar Tex^J Justificar^C Posición
^X Salir      ^R Leer fich.^\ Reemplazar^U Pegar txt ^T Ortografía^_ Ir a línea
```

Una vez modificamos el archivo, lo guardamos y reiniciamos el servicio NFS:

```
service nfs-kernel-server restart
```

En los equipos que funcionen como **clientes**, es decir, los que queremos que accedan a la carpeta compartida en el equipo servidor, simplemente debemos instalar el servicio de cliente NFS y posteriormente montar la carpeta compartida en un directorio deseado:

sudo apt-get install nfs-client

Para montar la carpeta compartida por ejemplo en /home/usuario/Escritorio, tipeamos:

```
mount  {Ip_servidor}:{ruta_origen} {ruta_destino}
```

Por ejemplo:

```
mount 192.168.1.2:/home/lapvirtual/Escritorio/compartida
/home/usuario/Escritorio
```

Se puede configurar de muchos modos un servidor NFS, ya que este sistema de archivos provee diversas funcionalidades, para profundizar se sugiere ver la documentación oficial de NFS para Ubuntu.

## Utilizando FTP

Podemos emplear el protocolo de transferencia de archivos FTP para poder intercambiar archivos con un equipo de nuestra propia red local o incluso con un servidor distante que se encuentra conectado a Internet. Esto es especialmente útil por ejemplo cuando queremos subir el contenido de un sitio web para publicarlo en Internet en un servidor de hosting, o si tenemos un servidor remoto de archivos desde el cual podemos realizar respaldo de nuestros datos, o bien si simplemente tenemos en nuestra red doméstica o institucional una serie de ficheros compartidos para toda la red.

Este protocolo, también funciona en modalidad cliente/servidor, es decir, para poder trabajar con él, si queremos que nuestro equipo actúe como servidor y que sean otros los que se conecten a él para acceder a los ficheros, entonces deberíamos instalar un software **servidor** FTP, mientras que si queremos que nuestro equipo acceda a un servidor remoto como cliente, debemos instalar el software **cliente.**

En Windows, existen varias aplicaciones que realizan esto desde una interfaz gráfica, como ser Filezilla, SmartFTP, Cyberduck, entre otros. También existen aplicaciones con interfaz gráfica en Linux, pero para que se conceptualice de mejor manera esto, veremos un ejemplo de cómo instalar un servidor FTP en Ubuntu desde la terminal, así como también cómo utilizar el cliente, siendo que en Linux ya lo tenemos instalado.

### Instalar el servidor FTP en Linux

Para instalar FTP en nuestro equipo servidor, simplemente debemos ejecutar desde una terminal, el instalador del paquete **vsftpd** con permisos de administrador, el comando sería:

```
sudo apt-get install vsftpd
```

Los parámetros de configuración del servidor se encuentran en el archivo /etc/vsftpd.conf, debemos abrirlo con un editor de texto, como por ejemplo el nano:

```
nano /etc/vsftpd.conf
```

Desde dicho archivo, podremos modificar las directivas para añadir seguridad a nuestro servidor, determinando qué direcciones autorizamos a entrar. El archivo debería tener un contenido similar al siguiente:

```
lapvirtual@lapvirtual-VirtualBox: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
  GNU nano 2.5.3              Archivo: /etc/vsftpd.conf

# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#

^G Ver ayuda   ^O Guardar     ^W Buscar      ^K Cortar Text^J Justificar  ^C Posición
^X Salir       ^R Leer fich.  ^\ Reemplazar  ^U Pegar txt  ^T Ortografía  ^_ Ir a línea
```

Por defecto, el servidor FTP solicitará autentificación al cliente para acceder en forma remota, es decir, el cliente deberá ingresar un nombre de usuario y contraseña válidos en el equipo servidor, no obstante, podemos habilitar el ingreso de usuarios anónimos (lo que debilitaría en gran medida la seguridad) modificando la directiva “anonymous_enable” que debería estar en “No”, quedaría:

```
anonymous_enable = Yes
```

En el mismo archivo, si queremos habilitar que los usuarios que ingresen puedan editar o subir archivos (además de sólo descargar) simplemente se debe cambiar la directiva write_enable:

```
write_enable = YES
```

Una vez que hemos terminado de configurar los parámetros del servidor FTP, debemos reiniciar el servicio, utilizando el comando:

```
sudo systemctl restart vsftpd.service
```

Por mayor información, se sugiere consultar la Documentación de Ubuntu

## Acceder a un servidor FTP desde un cliente en Linux

Desde la vista del cliente, el comando para conectarnos por FTP a un servidor es simplemente a nivel genérico “ftp {IP_SERVIDOR}”. Por ejemplo:

```
ftp 10.0.2.15
```

El sistema nos responderá solicitando el ingreso del nombre (nombre de usuario autorizado) y luego la contraseña. Después de loguearnos, el sistema ya cambia el prompt a ftp>, lo que nos da la pauta de que efectivamente estamos conectados. Si queremos subir un archivo al servidor, simplemente debemos usar el comando **send**, de la forma “send {ruta_archivo_origen} {ruta_archivo_destino}” como por ejemplo:

```
send /home/usuario/Escritorio/archivo.txt /home/servidor/Escritorio/compartida
```

A continuación se ve una captura de pantalla donde nos hemos conectado remotamente al servidor FTP y utilizamos el comando “**?**” para ver toda la lista de posibles órdenes que podemos ejecutar desde el cliente:

```
lapvirtual@lapvirtual-VirtualBox: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

lapvirtual@lapvirtual-VirtualBox:~$ ftp 10.0.2.15
Connected to 10.0.2.15.
220 (vsFTPd 3.0.3)
Name (10.0.2.15:lapvirtual): lapvirtual
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ?
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
account         exit            mget            put             status
append          form            mkdir           pwd             struct
ascii           get             mls             quit            system
bell            glob            mode            quote           sunique
binary          hash            modtime         recv            tenex
bye             help            mput            reget           tick
case            idle            newer           rstatus         trace
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
```

## Accediendo a un equipo remoto por SSH

SSH es un protocolo que como se habló en una sección anterior de esta guía, permite el control remoto de una computadora desde otra. Para poderse utilizar, la computadora de destino (la que queremos controlar) debe tener instalado el servidor SSH. Desde el cliente, sólo debemos saber la dirección IP de la computadora remota (servidor) y un usuario y contraseña para autentificarnos.

En el caso de utilizar Windows, existen varias herramientas para conectarnos por SSH, una de ellas es Putty, en el caso de Linux, al igual que pasaba con FTP, el cliente ya lo tendremos instalado, no así el servidor. Desde el equipo que deseamos que funcione como **servidor**, lo primero es instalar el servidor SSH, el comando es:

```
sudo apt-get install openssh-server
```

Luego de esto, podemos configurar los parámetros que queramos indicarle al servicio, desde el archivo /etc/ssh/sshd_config, por ejemplo con el programa nano:

```
nano /etc/ssh/sshd_config
```

Si lo dejamos por defecto, SSH operará en el puerto 22 de nuestro equipo. Simplemente debemos iniciar el servicio con el comando:

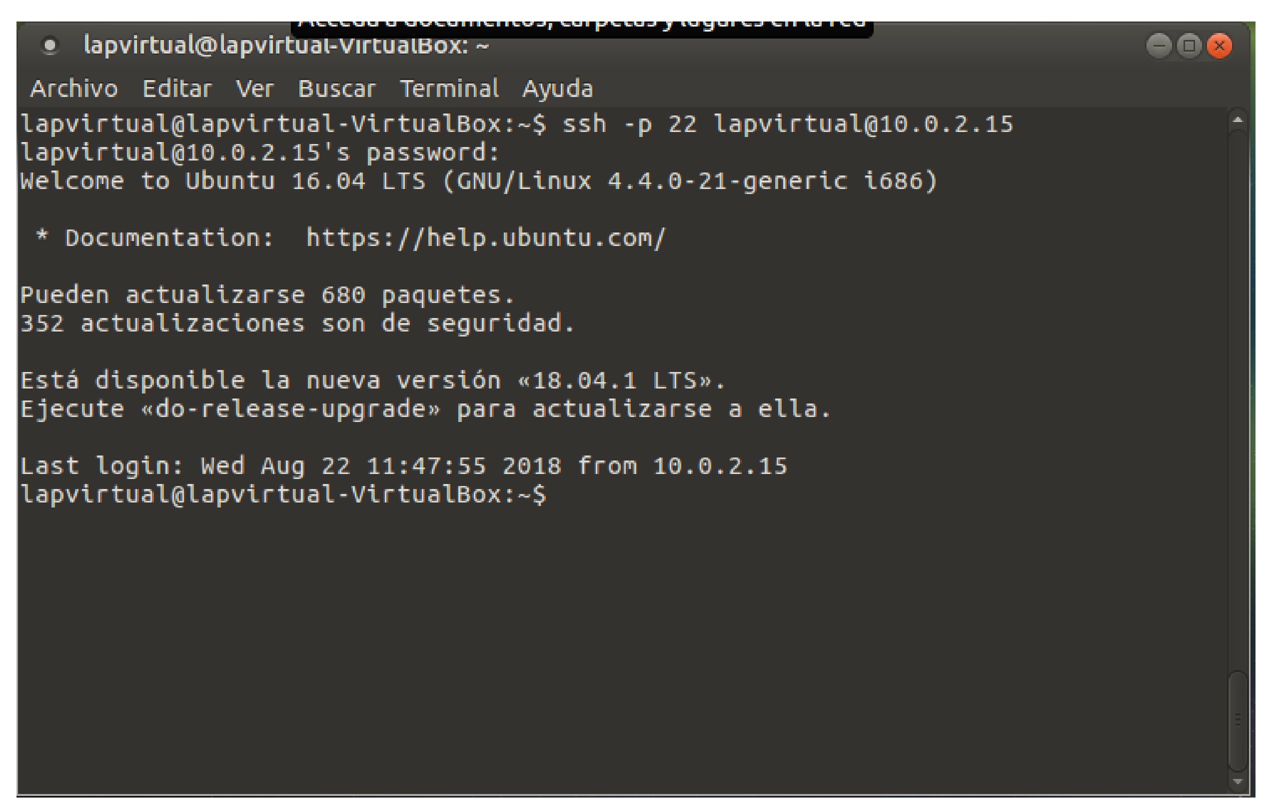
```
sudo /etc/init.d/ssh start
```

Si ya lo teníamos corriendo en el servidor e hicimos algunos cambios en el archivo de configuración, podemos reiniciarlo, utilizando el comando “restart” en lugar de “start”. Cabe aclarar que también podemos detener el servicio con el comando “stop”.

Desde el **cliente**, basta con utilizar el comando “ssh –p {puerto} {usuario}@{ip_servidor}. Por ejemplo:

```
ssh -p 22 root@10.0.2.15
```

El sistema nos pedirá autentificarnos con un nombre de usuario y contraseña autorizados en el servidor, y luego de eso ya podremos ejecutar por la terminal los comandos que queramos directamente hacia el servidor. En la imagen siguiente vemos cómo ejecutamos los comandos correspondientes desde un equipo llamado “lapvirtual” hacia un servidor con un usuario que lleva el mismo nombre, esto ocurre porque para el caso de ejemplo, se usan máquinas virtuales idénticas (pero esto no tiene por qué ser así, de hecho este es un caso excepcional):




Como siempre, para profundizar se sugiere consultar la [Documentación oficial de Ubuntu]

# Despedida

Si usted lector, es estudiante del curso de Taller de Mantenimiento del Bachillerato de Informática del CETP-UTU, o bien es docente y este material le ha servido de ayuda para llevar a cabo alguna tarea referente al curso, esta guía ya se puede considerar que ha cumplido con su propósito y le agradezco por haberla considerado.

Si en cambio usted, es un lector ajeno al mencionado curso, pero esta guía le ha servido de alguna ayuda, para comprender algún tema o para tener alguna idea general sobre algún tema en específico, al igual que en el caso anterior, puedo decir que esta guía ha cumplido con su propósito y le agradezco por haberla considerado.

Si usted se ha tomado el tiempo de leer esta guía sin saber nada sobre redes, y ahora tiene una idea global de lo que son las redes de computadoras, cómo se conforman y qué utilidades les brinda al usuario, puedo decir lo mismo que para los casos anteriores.

Si usted se ha tomado el tiempo de leer esta guía teniendo conocimientos sobre redes de computadoras y en algún aspecto encuentra algún error, de la naturaleza que sea, le agradezco por su tiempo y si lo desea, cualquier crítica constructiva para poder mejorarla y poder transmitir un material de mejor calidad. Al principio del texto podrá encontrar mi dirección de correo electrónico.

Sea el caso que fuere, deseo informar mi intención con este trabajo de simplemente ayudar y brindar un material de referencia, el cual en muchos casos se compone de citas de artículos de conocidos sitios web que pueden ser visitados desde Internet, pero que han sido previamente leídos y seleccionados por mí para componer parte del material, no sin referenciar la fuente de la cual se extrae el material copiado. A su vez, deseo informar a todo aquel que le interese utilizarla, distribuirla libremente a través de la red, imprimirla o incluso hacer modificaciones constructivas, aunque fuese con fines comerciales, siempre que se reconozca mi autoría en el trabajo original, también puede utilizarla y en lo personal es un gusto que el material le sea de utilidad. Sin embargo se aclara que, el propósito inicial de este trabajo es meramente educativo y con fines de que tenga la mayor difusión posible, de manera libre y gratuita.

# Bibliografía


- CISCO. (2004). CCNA1: Conceptos Básicos de Networking. México, México: Pearson.
- CISCO. (2016, 10 agosto). Direccionamiento de IP y conexión entre subredes para los usuarios nuevos. Recuperado 30 julio, 2018, de https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13788-3.html
- Comparación de los Modelos OSI y TCP/IP. (s.f.). Recuperado 30 julio, 2018, de https://www.uaeh.edu.mx/scige/boletin/huejutla/n10/r1.html
- Comunicación a través del puerto RS-232. (s.f.). Recuperado 30 julio, 2018, de https://tuelectronica.es/comunicacion-a-traves-del-puerto-rs232/
- Dayssy Payares y María Fandiño (Facultad De Ingeniería – Universidad Tecnológica de Bolívar, 2004), Conmutación, Enrutamiento y Tecnologías WAN.
- Frecuencia Modulada. (s.f.). Recuperado 30 julio, 2018, de https://www.ecured.cu/Frecuencia_modulada_(FM)
- IBM. (s.f.). Interfaces de Red TCP/IP. Recuperado 30 julio, 2018, de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/com.ibm.aix.networkcomm/tcpip_interfaces.htm
- Ing. J.Joskowicz (Instituto de Ingeniería Eléctrica –FING, 2013), Cableado Estructurado, Versión 11
- Isaías Torres Martínez. (s.f.). Direccionamiento de IP y conexión entre subredes para los usuarios nuevos. Recuperado 30 julio, 2018, de https://www.quia.com/files/quia/users/istomar/DIPS/index.html
- Modelo OSI: Niveles de Referencia. (s.f.). Recuperado 30 julio, 2018, de http://modeloosica.blogspot.com.uy/2016/03/niveles-de-la-referencia-osi.html
- Modulación AM. (s.f.). Recuperado 30 julio, 2018, de https://www.electronicafacil.net/tutoriales/MODULACION-AM.php
- Protocolos RIP/OSPF/BGP. (s.f.). Recuperado 30 julio, 2018, de http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/protocols.html
- Vega, C. Pérez. (s.f.). Magnitudes Logarítmicas. Recuperado 30 julio, 2018, de http://personales.unican.es/perezvr/pdf/CH2ST_Web.pdf

- Suárez, A. (s.f.). Conexión Null Modem. Recuperado 30 julio, 2018, de https://telematica2.wordpress.com/2011/02/18/conexion-null-modem-modem-nulo/)
- Tanembaum (2014), Redes de Computadoras, Quinta Edición
- Topologías de Red. (s.f.). Recuperado 30 julio, 2018, de https://csudp.wikispaces.com/file/view/Topologias+de+Red.pdf